Impact and Legacy of the COVID-19 related digital adoption on ISM On SMEs operating in Abu Dhabi

by

Mahra Mohammed Al Mulla

A thesis submitted in partial fulfilment for the requirements for the degree of Doctor of Business Administration (DBA) at the University of Lancashire

11/2025

University of Lancashire

RESEARCH STUDENT DECLARATION FORM

Type of Award Doctor of Business Administration (DBA)

School of Business

1. **Concurrent registration for two or more academic awards**

   I declare that while registered as a candidate for the research degree, I have not been a registered candidate or enrolled student for another award of the University or other academic or professional institution.

2. **Material submitted for another award**

   I declare that no material contained in the thesis has been used in any other submission for an academic award and is solely my own work.

3. **Collaboration**

   Where a candidate's research programme is part of a collaborative project, the thesis must indicate in addition clearly the candidate's individual contribution and the extent of the collaboration. Please state below:

   Not applicable

4. **Use of a Proof-reader**

No proofreading service was used in the compilation of this thesis.

Signature of Candidate

Print name: Mahra Mohammed Al Mulla

ABSTRACT

The emergence of coronavirus disease 2019 (COVID-19) affected Small and Medium-sized Enterprises (SMEs)' business continuity, hence the need to redefine Information Security Management (ISM) practices. This research aimed to analyse the impact of the post-COVID-19 digital shift on ISM practices in SMEs in Abu Dhabi through identifying risks and countermeasures to cyber threats. SMEs are significant for the United Arab Emirates (UAE) economy since 94% of the total number of businesses in the country and 86% of the private sector employee's work in SMEs (Singh, 2020). However, due to enhanced digitalisation of their operations, they are at high risk of cyber incidents including hacking and ransomware.

The present research contributes to the existing literature by conducting qualitative interviews with SME executives and cybersecurity professionals to understand the difficulties that SMEs experience and the steps required to improve ISM practices. Based on the Protection Motivation Theory (PMT), the study investigates the SMEs' cyber threat perception and response strategy in resource-scarce contexts, which enhances the theoretical contribution by integrating ISM with the digital resilience theory.

Practical contributions are the creation of an SME-specific best-fit ISM model, guidelines for the government-supported cybersecurity programmes, and the ways to adopt cost-effective and sustainable technologies. The study focuses on policymakers, IT solution providers and SMEs in the enhancement of digital preparedness for sustainable economic development of Abu Dhabi. With reference to cybersecurity readiness in SMEs during crisis-induced digital change, this research fills essential gaps in the literature while providing practical recommendations to enhance SMEs' readiness and contribute to Abu Dhabi's economic diversification.

Keywords: *Information Security Management, digital adoption, Cybersecurity, SMEs, COVID-19, Protection Motivation Theory, digital resilience.*

TABLE OF CONTENTS

ACKNOWLEDGMENTS

I would like to thank my supervisors for their help through their guidance, which was invaluable throughout the time I spent researching and writing this thesis. I would like to thank the University, in particular, the University of Lancashire Business School which has given me a supportive learning environment and facilities to work in order to complete this research. I would also like to thank my colleagues whose contributions to my learning have been invaluable. I would like to end by thanking my family members and friends for their unfailing support and continuous encouragement to me throughout the years of my study and the research and writing of this thesis.

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

Complete Term	Abbreviation
Association of Chartered Certified Accountants	ACCA
Association for Computing Machinery	ACM
Abu Dhabi Chamber	ADC
Abu Dhabi Digital Authority	ADDA
Abu Dhabi Department of Economic Development	ADDED
Advanced Encryption Standard	AES
Artificial Intelligence	AI
Application Programming Interface	API
Amazon Web Services	AWS
Business Impact Analysis	BIA
Business Continuity Planning	BCP
Computer-Aided Facilities Management	CAFM
Cloud Access Security Brokers	CASB
Chief Executive Officer	CEO
Cybersecurity for Humans against Illegal and Non-digital Lives	CHILD
Critical Information Infrastructure Protection	CIIP
Centre for Internet Security	CIS
Coronavirus Disease 2019	COVID-19
Cyber-Physical Systems Security	CPSS
Computer Reseller News	CRN
Cybersecurity Framework	CSF
Cybersecurity Operations	CSO
Cloud Service Provider	CSP
Distributed Denial of Service	DDoS
Data Loss Prevention	DLP
Digital Resilience Theory	DRT
Enterprise Resource Planning	ERP
File Transfer Protocol	FTP
Gross Domestic Product	GDP
General Data Protection Regulation	GDPR

Gulf Information Security Expo and Conference	GISEC
Health Information Trust Alliance	HITRUST
Heating, Ventilation, and Air Conditioning	HVAC
UAE Information Assurance Regulation	IAR
International Chamber of Commerce	ICC
Information and Communication Technology	ICT
Intrusion Detection Systems	IDS
Intrusion Detection and Prevention Systems	IDPS
Internet Protocol / User Datagram Protocol / Transmission Control Protocol	IP / UDP / TCP
International Professional Practices Framework	IPPF
Information Systems Auditor	ISA
Information Security Management	ISM
International Organization for Standardization	ISO
Internet of Things	IoT
Key Performance Indicator	KPI
Multi-Factor Authentication	MFA
Multi-Variant Execution Environments	MVEE
National Cybersecurity Strategy (UAE)	NCS
National Electronic Security Authority	NESA
National Institute of Standards and Technology	NIST
Organisation for Economic Co-operation and Development	OECD
Protection Motivation Theory	PMT
Secure Access Service Edge	SASE
Software-Defined Networking	SDN
Small and Medium Enterprises	SMEs
Secure Sockets Layer	SSL
Standard Operating Procedures	SOP
Technology-Organization-Environment Framework	TOE
United Arab Emirates	UAE
Universal Serial Bus	USB
Virtual Desktop Infrastructure	VDI
Virtual Private Network	VPN

CHAPTER 1: INTRODUCTION

1.1 Introduction

Small to Medium Enterprises (SMEs) are an essential part of the global economy and faced several challenges, including weak performance, reduced revenues, employment issues, and remote-work-related to Information Security Management (ISM) challenges during the COVID-19 period (Anderson, Ahmad and Chang, 2024; Mishrif and Khan, 2023). SMEs are among the most strategic and focused sectors in the UAE as they are the pillars of boosting and diversifying the economy, as of 2020, there were approximately 350,000 SMEs (UAE, 2022).

According to Singh (2020), among the total number of companies, more than 94 % are SMEs in the UAE employing approximately 86% in private sectors contributing to more than 50% of the total non-oil GDP. A report published by the Abu Dhabi Chamber (ADC, 2019) aligned with these findings and stated that 43% of employees in Abu Dhabi received salaries from companies categorised as SMEs in 2019. The research on SMEs during and post-COVID has increasingly focused on their digital adoption by SMEs as a source of employment while the performance of these SMEs was impacted significantly during the pandemic (Kumar and Ayedee, 2021). Papadopoulos et al. (2020) showed that the digital adoption in SMEs, though accompanied by reluctance, has increased during and post COVID-19 and thus requires proper Information Security Management (ISM).

The study focuses on digital adoption which as defined by Kumar and Ayedee (2021), is the process where individuals or organisations integrate digital technology and tools into daily activities. The term "digital adoption" refers to the level to which those businesses apply digital technology and tools in daily operations. Indeed, SMEs have increasingly embraced digital solutions to expedite their operations, enhance their competitiveness, and explore the increasing availability of digital tools and technologies. This has been driven by numerous factors: the need to keep up with shifting customer expectations and compete with their digital-native rivals. The COVID-19 epidemic forced the SMEs to learn how to work with employees remotely using virtual channels of communication. This accelerated their adoption of digital technologies accordingly.

The adoption of digital technology within SMEs is evident in many forms (Abuhussein, Barham and Al-Jaghoub, 2023). For instance, SMEs may adopt digital techniques that will improve their marketing and interaction with their consumers through effective marketing campaigns using social media or emails. They could also leverage digital technologies in automating their internal activities relevant to their business strategy, including accounting or inventory management (Wendt et al., 2021). Cloud-based services, which means that firms have the capability to store and access their data and

applications online rather than holding them on local servers, may be also part of the process of digital adoption.

Other studies conducted by Dwivedi et al. (2020) and Akpan et al. (2022) showed the stability of results in line with the findings from the research of Papadopoulos, Baltas and Balta (2020). According to Ikmal et al. (2020), Abu Dhabi SMEs are at four times higher risk and tend to suffer from crises and shocks due to lack of resources and may have an 8 % higher likehood to close the business or stop the activity than large enterprises. Similar findings were demonstrated by Zarrouk et al. (2020) who presented that business performance is significantly affected due to COVID-19. This notion is evidenced in the survey conducted by Cybereason (2021) stating that about 42% of businesses in the UAE shut down their business after experiencing a cyberattack. Table 1-1 is provided below showing the breakdown of businesses in different countries and the number of firms that had to shut down their businesses. It was observed from the reported data that UAE is among the most affected country followed by the UK and US where 34% and 31% of businesses closed their business operations after a cyberattack.

Table 1-1: Business Closure by Region due to cyberattacks, Source: (Cybereason, 2021) Source: Self-made

Region	Percentage Reporting Business Closure due to Cyberattacks
UAE	42%
UK	34%
USA	31%
France	22%
Germany	21%
Singapore	20%
Spain	5%

The survey included 1,263 professionals in the cybersecurity field from different countries such as UAE, UK, USA, Spain, France, Germany, and Singapore working in various industries such as manufacturing, finance, technology, etc. An article written by Abbas (2021) and published in Khaleej Times discussed the findings of the Cybereason survey and stated that businesses paying ransom money in the UAE are about 28%. The companies paid huge amounts to regain access to the systems in the post-cyberattacks. In addition, it was noticed that companies also closed their operations after the ransomware attack. The report highlighted that about 90 % of the companies who already had paid huge payments again suffered from the attack of ransomware mostly from the same threat group (Abbas,

2021). Thus, the current study aims to analyse the legacy and impact of COVID-related digital adoption on the ISM in the SMEs of Abu Dhabi.

1.2 Background

Cybersecurity, as revealed by Seemma et al. (2018), is referred to as the techniques and methods used to protect and secure the cyber-environment of an organisation or business users. In this essence, Information Security Management (ISM) can be considered a vital part as cybersecurity involves a wide range of collection of policies, concepts, risk management approaches, and practices (Solms and Niekerk, 2013). Data security means that no unauthorised access or data breach can be attempted against an organisations or an individual's digital information all along its lifecycle (Bandari, 2023). Cybersecurity and data security have shown numerous developments over the last few years in the UAE businesses, especially SMEs had to transform and adopt digital technologies to cope with the post-COVID-19 period (Idir, et al., 2021).

The COVID-19 pandemic has had a profound impact on businesses around the world, forcing many to adapt quickly to new ways of working and engaging with customers. One of the most significant changes has been the rapid increase in digital adoption among SMEs, as businesses have had to pivot to remote work and digital communication to maintain operations.

Before the epidemic, a large number of SMEs were already examining ways they could improve their activities using digital tools and technologies (Indriastuti and Fuad, 2021). However, the COVID-19 crisis accelerated this trend since businesses have to shut down physical premises and find new ways of serving customers using these new methods. This is the case because of the obligations for businesses to close and transfer business entirely.

The need to work from home and communicate virtually has contributed to increased digital tools being used in the wake of the COVID-19 pandemic (Riemer et al., 2020). This is attributed to the fact that businesses were compelled to find new ways of communicating with both their employees and customers. Among the key elements of digital adoption, utilization of online marketplaces and e-commerce reportedly gained most attention among SMEs (Apriani et al., 2024). Many SMEs sell their products on online marketplaces such as Amazon and Etsy, as traditional stores are closed or opened under restrictions (Pinzaru, Zbuchea and Anghel, 2020). Even during the peak of the pandemic, this has allowed businesses to keep generating revenues by reaching out to a wider audience and continuing their operations as usual. The other sector in which wide adoption of digital technology has been seen is the use of virtual communication and collaboration tools.

With time, many workers have begun to stay home and work, a trend which organisations now have to adapt to and devise new means of keeping the employees inter-connected to ensure the job is actually

being done properly (Golinelli et al., 2020). Due to this, there has been an observed rise in the utilization of video conferencing tools such as Zoom and Microsoft Teams and collaboration platforms. Not surprisingly, cloud-based services have grown increasingly popular with SMEs too, which sought ways to store data and apps online and access them rather than on their own local servers. Cloud-based solutions and Web Services gave SMEs the needed scalability and flexibility to quickly respond to the changing market conditions and the demands of their customers. Meanwhile, the increase in digital adoption by SMEs has not been devoid of challenges (Pinzaru, Zbuchea and Anghel, 2020).

The move to digital has highlighted various weaknesses in IT architecture and security for many of the SMEs. This sudden and unseen upsurge in work in home environments spaced apart and the virtual communication system compelled SMEs to rapidly adapt to fresh security risks and evolving threats (Baig et al., 2020). This introduction of new vulnerabilities makes SMEs more exposed to cybersecurity attacks and possible data breaches. Worries also exist regarding the effects that rapid digitalisation will have on staff and the culture of organisations. In particular, the surge to remote working and virtuality in communication seems to be eroding the traditional working practices that might have a considerable effect on staff welfare and job satisfaction (Riemer et al., 2020). Even when working in a virtual setting, SMEs will need to develop innovative approaches to employee management in order to keep their workers supported and engaged (Riemer et al., 2020).

Cybersecurity and ISM have become essential as SMEs are increasingly becoming digital, the cybercrimes are rising in the UAE and worldwide as threats like ransomware have stressed the significance of data security (Rizvi, 2022). The trends regarding cybersecurity in UAE suggest that the Middle East region is experiencing a *'cyber pandemic'* after the COVID-19 related digital adoption by SMEs is being exploited exponentially by hackers (Murphy, 2020). The current study is based on exploring the ISM and cybersecurity practices by SMEs to reveal the challenges and produce solutions for the SMEs in Abu Dhabi.

According to an article written by Altaher (2016), there has been a 500 % increase in cyberattacks on UAE as the country moves towards digitalisation making it a potential target of 5% of global cyberattacks. In agreement with this, the paper written by Guven (2018) stated that digital adoption in consumers, economic growth of the country, and high social media penetration are factors involved in making UAE a potential target for cyberattacks. A report published by Help AG / Etisalat (2021) found that *"Distributed Denial of service attack (DDoS)"* attacks on small businesses within UAE increased by 183% in 2020 compared to previous years, thus the situation is also found to be risky for SMEs across the UAE. The report's findings are based on the observations of DDoS protection services provided by Help AG / Etisalat within the UAE, Hussain (2021) discussed that DDoS cyberattacks can rapidly and easily corrupt SMEs' business networks and disrupt their business transactions. The study by Ahmed

and Nanath (2021) highlighted that SMEs' weak infrastructure and loopholes in the defence mechanism attract hackers to conduct cyberattacks on them. Therefore, it was observed that SMEs lack resources to prevent cyberattacks in the form of viruses, malware, phishing, intrusion, denial of service (DoS), data theft, and other attacks (OECD, 2019).

The problem of vulnerability of SMEs in Abu Dhabi and UAE has increased and requires the attention of scholars and practitioners (Costa and Castro, 2021). This is due to the reason that economy of the countries is also dependent on the growth of the companies including SMEs and large size organisations (Sergi et al., 2019; Al Aina and Atan, 2020). However, there is little focus on exploring the challenges of SMEs and how they can overcome these issues. As the SMEs in Abu Dhabi moved to digital operation, the shift to remote-working produced vital security challenges and concerns and exposed business-sensitive information to DDoS, ransomware, and other cyberattacks (Malecki, 2020).

A report published by OECD (2016) analysed the business market in Abu Dhabi and declared that SMEs density is lower, although entrepreneurial intentions are strong fewer entrepreneurial actions are examined. Nevertheless, SMEs are vital for economic diversification in Abu Dhabi to avoid high dependence on an oil-based economy and increase the economic activity of SMEs which is currently 29% of the total GDP (ADC, 2019). The study by Hassib and Shires (2022) demonstrated that SMEs have greatly been impacted by the rapid digitalisation during the pandemic for business continuity increasing vulnerabilities towards various cybersecurity issues. In agreement with this study, Alshehhi (2017) and Klein and Todesco (2021) also argued that prompt adoption of digitalisation in SMEs enhanced the challenges in terms of the performance of the businesses due to cybersecurity issues.

Correspondingly, an official report by Interpol (2020) indicated that the pandemic impacted the severity of the threats with an increase in disinformation, online fraud, and cybercrimes. The report included findings of research conducted by Trend Mirco (2020), one of Interpol's partners, indicating about 907,000 spam messages, 48,000 malicious links, and 737 malware attacks related to COVID-19 were determined and blocked in 2020. According to Mrad (2021) among the cyberattacks in UAE related to the pandemic, account compromise was among the foremost that impacted about 28%, followed by phishing attacks harming 20%, and inside attacks damaging 17% of the total SMEs. A recent publication indicates a 71% increase in UAE cyberattacks whereas a global increase of 50% is examined worldwide cyberattacks (Zawya, 2022). As cyber threats are increasing and technologically advancing, studies (Maher, 2022; Al-Sharji, et al., 2021) suggest that SMEs in Abu Dhabi should closely evaluate and monitor their cybersecurity and IMS practices.

1.2.1 Key constructs

Digital Adoption: It is a process where SMEs adopt and integrate digital technologies, including cloud computing, remote platforms, and digital payment system, to improve efficiency, customer access, and competitiveness (OECD, 2021).

Information Security Management (ISM): An organised strategy that incorporates individuals, processes, and technology to ensure the protection of information assets through the implementation of risk management and control processes (ISO/IEC 27001:2013).

Small and Medium Enterprises (SMEs): Organisations with fewer than 250 employees and marked by limited financial and technological capabilities but high levels of adaptability and innovation ability (Abu Dhabi Department of Economic Development, 2023).

1.3 The rationale of the study

As the world economy shifts and transitions are witnessed in the way businesses are conducted, the success factors of businesses transfer from concrete to fragile assets (Ključnikov, et al., 2019). The study by Pu et al. (2021) also showed agreement with the findings of this study. In this regard, Isachenko (2018) demonstrated that among intangible assets, information becomes one of the most important and valuable assets of SMEs. A report published by Ponemon Institute, (2018) claimed that high-value information assets are private and confidential to the organisations and a data breach would lead to damage requiring costly mitigation and other grave consequences such as loss of share in the market. For instance, Equifax spent about 1.4 billion dollars to clean up after a cyberattack incident including the cost of technological transformation for improvements in networks, applications, and security of information and business data (Sharma, et al., 2020). According to Pancholi and Strobl (2019), the survey results based on 597 companies in Europe suggested that digital transformation is associated with cyber risks and increases the exposure of business-sensitive information to hackers.

As COVID-19 hit the world, all businesses including SMEs had to adopt technological advancements to continue operations and transactions. Shouk and Eraqi (2015) highlighted the aspect that SMEs' readiness for digital adoption is limited, and they are reluctant to adopt online technologies mostly because of a lack of resources and human capital. Conversely, owing to the market demands a wide range of studies (Shouk and Eraqi, 2015; Lin, et al., 2019) suggest majority of SMEs have shifted towards digital adoption and e-commerce during the pandemic. Kljucnikov et al. (2019) argued that digital adoption is likely to facilitate the growth of the digital economy, but the use of the Internet and Information and Communication Technologies (ICT) is closely linked to threats.

According to Costa and Castro (2021), the ever-increasing digital adoption in SMEs during and post COVID-19 has gained attention from scholars as they critically evaluate information security

management practices, and strategies and anticipate desired policy behaviour. The same practices were highlighted by Bai et al. (2021) considering the post-COVID period. There is a need to critically evaluate ISM practices and strategies in SMEs of Abu Dhabi to analyse its cybersecurity measures and challenges. As this will help the SMEs to handle the same issues if encountered by the organisations in the future. In addition, the SMEs in other regions of the UAE can also adopt these measures and solutions to resolve the cybersecurity issues of ISM to enhance the performance of the organisation.

1.4 Research Aim and Research Objectives

The aim of the study is to analyse the impact of post-COVID digital adoption on ISM in SMEs of Abu Dhabi. The objectives are as follows.

i. To critically evaluate the information security practices in SMEs in the wake of the COVID-19 pandemic in Abu Dhabi.
ii. To conceptualise the information security challenges in SMEs in the wake of the COVID-19 pandemic in Abu Dhabi.
iii. To identify and evaluate the tools and solutions addressing the information security challenges while adopting COVID-19 related digital practices.
iv. To critique options for addressing the SME cyber challenges with the development of an associated model for best practice.

1.5 Research Questions

The major research questions to progress the investigation are stated follows:

i. How has the digital adoption driven by COVID-19 impacted the information security management practices in the SMEs in Abu Dhabi?
ii. What strategies, tools and frameworks can effectively address the cybersecurity challenges faced by SMEs in Abu Dhabi during the COVID-19 digital landscape?

This paper is specifically concerned with small and medium enterprises (SMEs) in Abu Dhabi, as opposed to the UAE in general, because of the unique economic set-up and digitization path in the emirate. Abu Dhabi is a case of representation and strategic importance since it contributes to a significant portion of the SME sector in the UAE and functions within a distinct policy and innovation environment spearheaded by the Abu Dhabi Digital Authority (ADDA) and the Abu Dhabi Department of Economic Development (ADDED). These organisations have been the first to establish geo-specific cybersecurity, digitalisation, and SME support models in line with the Abu Dhabi Economic Vision 2030, which focuses on sustainable diversification via technology-based growth. In turn, Abu Dhabi offers a topical and policy-intensive environment to study the influence of government-initiated digital projects on the maturity and resilience of information security management (ISM) in SMEs. Although

the results are placed within the Abu Dhabi context, they can be regarded as reflective of the overall trends in the digitalisation of the SME sector in the UAE (ADDED, 2023; UAE Cyber Security Council, 2022; Rose et al., 2020).

1.6 Research Significance

The aim of the ISM is to enable, control, examine, improve and maintain the security of the information in the organisation while managing threats and risks such as cyberattacks and intrusion (Radu, 2018). The report compiled by Hau et al. (2016) stated that many SMEs remain unaware for months after they have been attacked. FireEye (2016) determined that media highly focus on cyberattacks on large enterprises whereas about 77% of cybercrimes are associated with targeting SMEs. Ahdadou et al. (2022) also highlighted the cybersecurity issues faced by SMEs.

As documented by Isachenko (2018) and Huyghue, (2021), information security was and would be a relevant and significant issue as information eliminates doubt and uncertainty regarding knowledge of some phenomenon. Furthermore, Merritt (2021) stated that ISM in SMEs is necessary because a lack of security can lead to damages impacting all stakeholders or a complete shutdown of the business in worse scenarios. For instance, the lack of security resulted in the breaching of the important information of the company and may lead to the loss of a huge amount for the employers. The customers are also affected, and their trust issues are increased due to poor services provided by the company due to leakage of their personal data from the system (Alferidah and Jhanjhi, 2020).

Aligning with this argument, Vadiveloo et al. (2016) discussed that 93% of the SMEs who faced a cyberattack experienced severe impacts to the business whereas 60% of SMEs closed down within 6 months of the attack. The same challenges were reported in the study of Mantha and de Soto (2019). Moreover, Arroyabe and Arroyabe (2021) declared that a cyberattack does not only impact the information system (IS) in SMEs but also affects in terms of reputation, the aftermath to supply chain, legal aspects, and business continuity. He et al. (2020) depicted that cybersecurity issues significantly influenced the innovation sector of the business that strongly affected the performance of the businesses and their financial success.

The study by Cheung et al. (2021) highlighted that cybersecurity issues affect the supply chain operations due to data leakage that also affects the performance and productivity of the companies. In agreement with the mentioned studies, Couce-Vierira et al. (2020) also highlighted that cyber threats and breaches impact stakeholders and produce implications regarding the correct management of information among shareholders and customers. On the contrary, the study by Ali (2021) stated that companies who are cyberattacked are liable to pay a fine to the UAE government which is likely to damage the company’s economic situation and reputation in the market.

According to the data, UAE companies encountered the issue of data breaching and not addressing the regulations to file the complaints bearing a fine of about 23 million US dollars to 28 million US dollars (Younies and Na, 2020). These findings demonstrated that cyberattacks impact organisations, their working, reputation and continuity of work to a higher extent. Further, a survey conducted by Cybersecurity Operations (CSO) in 2017 predicted that global cybercrime-related damage is expected to reach 6 trillion US dollars annually by 2021 (Nadeau, 2017). The survey included 510 respondents working at upper-level positions across different industries and public sectors worldwide. Farouk (2017) stated that the prediction of Nadeau (2017) is not surprising as cyber theft is to become the largest crime worldwide as indicated by the rapid rates of cybercrimes.

According to recent studies including Merritt (2021), Couce-Vierira et al., (2020) and Vadiveloo et al., (2016), the strengthening of cybersecurity in SMEs is critical for business operations, continuity, legal standpoint, company reputation, and the role played in the economic growth of the UAE. Simultaneously, this aspect also highlights the importance of studying the impact of COVID-19 related digital adoption on the information security management of SMEs in Abu Dhabi. The associated reason is that information security issues adversely impact the performance of the organisations by reducing their operations (Kljucnikov et al., 2019). In addition, this aspect has been a focus of the study focusing on the large-sized organisations while neglecting the challenges faced by the SME.

1.7 Contribution to Knowledge and Practice

Knowledge production and sharing imply that alternative explanations of change and transformation are likely to shape the understanding of a social phenomenon (Mitlin et al., 2019). This research contributes to the necessary knowledge and research by producing information on security practices evaluation in SMEs as they will be essential for sustaining digital adoption in the wake of COVID-19.

Knowledge is among the key resources that Mazdar (2018) believed could be used to inform practice to realize aspects of competitiveness in diverse areas. The study can also help in identifying the particular information security challenges faced by SMEs in Abu Dhabi; hence, the insights provided will be valuable for businesspeople, policymakers, and even researchers. The enterprises can prevent the improvement of information security practices, and the policymaker can come up with better policies and guidelines that will further support SMEs throughout the region once they could have profound understanding of the problems besetting the SMEs (Gani and Fernando, 2023; Moşteanu, 2020). It also helps in unearthing and determining the utility and mechanisms SMEs are applying to curb the challenges on information security that they are facing (Andraško, Mesarčík and Hamuľák, 2021).

This study also offers useful insights into other SMEs in the region and the IT solution providers, as they might be in a position to develop appropriate solutions to address these concerns after being apprised

of the information. Conclusively, this research contributes to more general discussions on the role of digital technology in business processes, which recently have gained relevance within the context of the COVID-19 pandemic. It would, therefore, inform broader discussions about the benefits and risks of digital technologies, strategies for managing these risks in the fast evolution of business environments, if it were able to understand the impact digital adoption has on information security practices in SMEs.

1.7.1 Contribution to Theory

This research contributes to the existing knowledge of ISM in SMEs by integrating Protection Motivation Theory (PMT) to examine the impact of the digital transition following the COVID-19 pandemic. The use of PMT in this particular case offers a good insight into the psychological and motivational aspects that affect the SME leaders in responding to cyber threats. As the potential threats in Abu Dhabi have escalated in the new normalcy period, particularly in the cyber domain, this study is highly applicable. Cybersecurity risks have been a concern for organisations globally, but the SMEs in the UAE and Abu Dhabi have been further challenged due to the increase in digital adoption due to the pandemic. While trying to adapt to long-term remote work, digital platforms, and e-commerce, the SMEs faced more security threats than before for proper security management.

The use of PMT in this research is essential since it has mainly been used in large enterprises or a single user to determine the decision-making process of specific cybersecurity measures. However, the studies in applying PMT to SME leaders in the context of cybersecurity are scarce, particularly in the economically strategic area of the UAE. The COVID-19 crisis has become an unprecedented event in which organisations, especially SMEs, had to quickly adopt digital business models. The rapid transition that has been experienced in the business environment has been crucial for the continuity of operations while bringing new risks and increasing the significance of protective measures. Using PMT, this research explores how SMEs managers in Abu Dhabi have addressed these threats regarding SMEs cybersecurity mainly on their perception of risk, self-efficacy and response efficacy.

The introduction of PMT into the research on cybersecurity in SMEs in Abu Dhabi contributes to the existing literature by encapsulating the psychological factors that influence decision making in the risky digital security contexts. The SME leaders' reaction is not only rational or technical, but it is also cognitive and depends on the perception of threat, control, and outcome. This research advances the knowledge on cybersecurity management in SMEs by focusing on the human factor that is a critical aspect of security measures.

Moreover, PMT will be employed in this research due to the recent calls for more attention to behavioral theories in explaining organisational reactions to cybersecurity threats. Although technology plays a significant role, it is not sufficient if accompanied by the lack of leadership commitment, staff

awareness, and the security culture in an organisation. This theoretical contribution therefore brings out a new perspective that integrates behavioral science into cybersecurity management in SMEs in a way that reinforces the conventional technical oriented and policy-based approaches.

Further, the utilization of PMT in the UAE context contributes to the existing literature culturally. It discusses the key issues related to the Abu Dhabi SMEs with references to the UAE's dependence on the digital transformation, the rising popularity of remote work, and the continuous development of cybersecurity in the country. The UAE is an economic and digital hub for the region and so this research provides insights into the Middle Eastern cybersecurity environment and best practices for both practice and policy.

1.7.2 Extending the Application of PMT

The current study indicates the applicability of PMT in determining how SME leaders perceive cyber threats and adopt ISM practices in the context of Abu Dhabi SMEs. Therefore, this study identifies motivational factors that create perpetuation of protective behaviour, perceived severity and perceived vulnerability, for which future studies can use PMT to extend its application to SME cybersecurity strategies.

1.7.3 Exploration of Digital Adoption Frameworks

In emerging economies, the exploration of digital adoption frameworks forms a part of the contribution to the literature of digital adoption theoretical frameworks, focusing on how rapid, crisis-forced digital transformations affect smaller enterprises. This is especially important within the context of an emerging economy like the United Arab Emirates, where SMEs are notably major contributors to GDP and employment. The results of this study will, therefore, be useful in building a framework that addresses only crisis-forced digital adoption and information systems management in resource-constrained environments.

1.7.4 Bridging ISM and Digital Resilience Theory

In this work, the Protection Motivation Theory (PMT) is used as the main theoretical framework, which helps to understand how the perceptions of cyber threats (threat appraisal) and the beliefs in the ability to deal with them (coping appraisal) as the perceptions of the SME leaders affect information security decision-making. Digital Resilience Theory (DRT) is used as the second or outcome-focused framework and is complementary to Digital Resilience Theory and refers to the way motivated protective behaviours develop into adaptive, sustainable and learning-based digital resilience over time (Rose et al., 2020). PMT therefore answers the question of why SMEs protect, whereas DRT answers the question of how SMEs move through the process of reactive security cultures to proactive security cultures as they engage in a process of learning and adapting.

Analysing ISM in the post-COVID period, the study contributes to the greater understanding of digital resilience in the context of SMEs. The research provides insight into how ISM practices influence the capabilities of SMEs to resist and adapt to cybersecurity threats. It places ISM in conjunction with digital resilience theory, which up to now has been mainly explored in greater enterprises and government sectors, hence providing a new approach toward SME resilience in times of crisis.

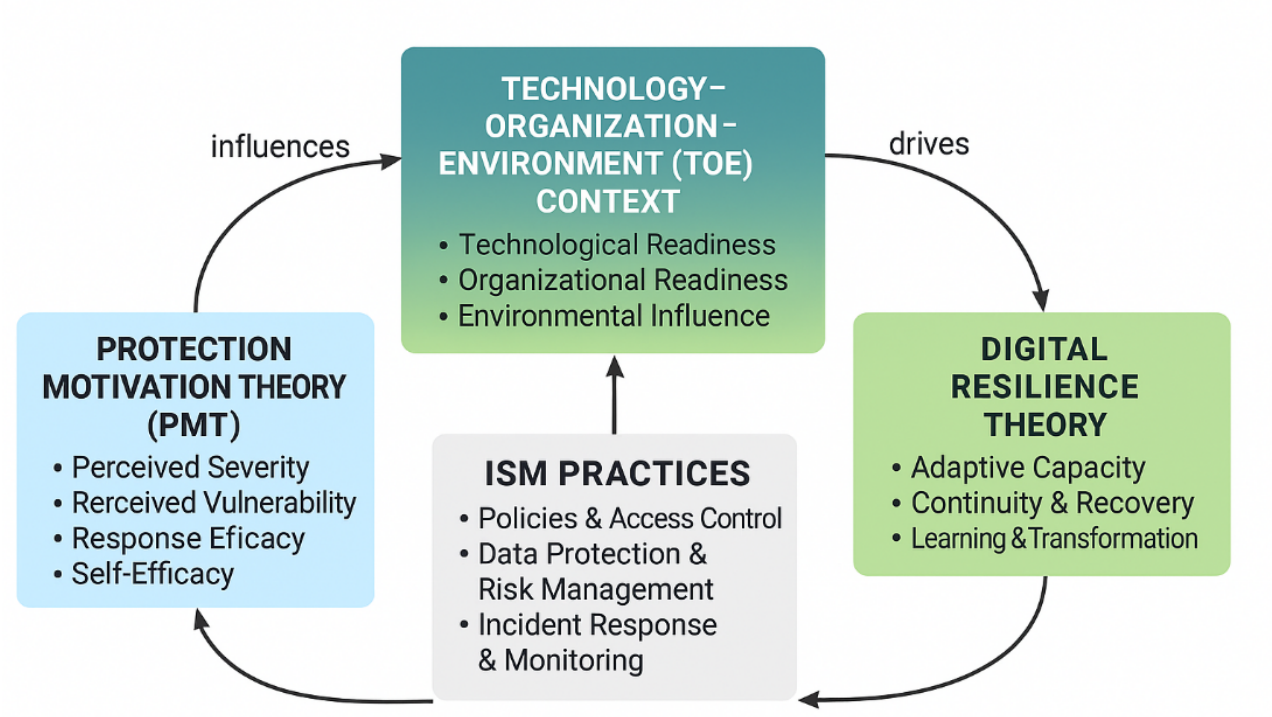

Figure 1-1: Linkage between PMT, Digital Resilience, and ISM in SMEs. Source: by author

Source: Author-developed conceptual linkage based on Protection Motivation Theory (Rogers, 1983), Technology–Organisation–Environment framework (Tornatzky and Fleischer, 1990), and Digital Resilience Theory (Rose et al., 2020; UAE Cyber Security Council, 2022). The diagram illustrates how cognitive motivation (PMT) and organisational readiness (TOE) jointly influence ISM practices, leading to digital resilience in SMEs.

Figure 1-1 show the connection between Protection Motivation Theory (PMT), Technology-Organisation-Environment (TOE) framework and Digital Resilience Theory (DRT) applied in the context of small and medium enterprises (SMEs) in Abu Dhabi. The model is a conceptualisation of the interaction between individual and organisational factors with information security management (ISM) practises and digital resilience in general.

On the left, PMT is used to indicate the cognitive-behavioural layer, which clarifies that perceptions of threat severity, vulnerability, response efficacy, and self-efficacy by the SME decision-makers influence their motivation to engage in secure practises (Rogers, 1983; Bada and Sasse, 2015).

The behavioural intention can be transformed into practical adoption in the presence of the TOE framework, which offers the structural-enabling context with the help of technology availability, organisational culture and regulatory environment (Tornatzky and Fleischer, 1990; Ahdadou et al., 2022).

The main ISM practises element serves to provide the working interface between motivation and outcome. It involves designing and implementing the security policies, data protection systems, access control and risk management procedures (Peltier, 2016). On the right, Digital Resilience Theory describes the results of such combined actions-increased adaptability, business continuity, and active recovery capability in the case of cyberattacks (Rose et al., 2020; UAE Cyber Security Council, 2022).

The blue-green gradient represents the change in the motivation preparedness to organisational strength. The Digital Resilience and PMT feedback loop means that there is a continuous learning cycle, which strengthens a culture of constant awareness and adaptive ISM maturity among SMEs.

1.8 Contribution to Practice

This study also provides practical insights that might help SMEs, policymakers, and technology providers in bringing improvements regarding ISM practices. These findings could guide SMEs in Abu Dhabi and other similar contexts toward effective cybersecurity measures and toward adapting ISM strategies that particularly respond to the challenges of rapid digital adoption. More specifically, the following practical contributions are highlighted:

1.8.1 ISM framework for SMEs

The proposed research sets out an overall ISM framework for SMEs by targeting resource-effective solutions. It includes best practices, tools, and processes that will be adopted by SMEs to protect digital assets, minimize cybersecurity risks, and ensure business continuity. This framework will indicate affordable and scalable ISM solutions to address financial constraints being faced by most SMEs.

1.8.2 Policy Recommendations for SME Cybersecurity

By identifying the most frequent security challenges faced by SMEs in Abu Dhabi, the study provides insights for policymakers to undertake focused interventions with regard to SME cybersecurity. A few policy recommendations might be government-funded cybersecurity training, public-private partnerships to provide SMEs with access to affordable cybersecurity tools, and regulatory frameworks that encourage businesses to adopt robust ISM measures.

1.8.3 Guidance for IT Solution Providers

The study has detected some key findings on the ISM needs of the SMEs, which can be used by IT solution providers in order to develop customized cybersecurity products and services. On the other

hand, the present research emphasizes certain specific vulnerabilities and gaps in ISM practices of SMEs and encourages IT providers to develop solutions based on those problems, such as affordable cloud security services, managed cybersecurity services, and easy-to-use monitoring tools suitable for SMEs.

1.8.4 Improved strategies for digital adoption

The study also highlights the need for resilience to ensure digital adoption among SMEs. The research canvasses some actionable strategies for SMEs to remain safe in the digital space, and this would go a long way to inform SMEs on how they could adopt secure practises in the usage of remote work tools, cloud services, and e-commerce platforms. This includes recommendations concerning the adoption of robust authentication protocols, regular cybersecurity training, and data encryption for sensitive information.

1.8.5 Wider Contributions to COVID-19 Recovery

This research furthers the global conversation on post-pandemic recovery for SMEs by highlighting further the role of cybersecurity for operational continuity. In a world economy still struggling to turn the effects of COVID-19, findings from this study suggest that SMEs could be playing a very important role in economic recovery if they can manage effectively risks in cybersecurity from digital adoption. This positions SMEs not as mere participants in recovery but resilient drivers of economic growth, capable of withstanding and adapting to evolving cybersecurity threats.

The research interest is sparked by the realisation that many Small and Medium-sized Enterprises (SMEs) express fear and reluctance towards adopting advanced technologies due to information security threats (Zutshi et al., 2021). Based on this interest, it is clear that small and medium-sized businesses (SMEs) do not have a strong defence against cyber risks because they lack the necessary knowledge and resources.

This research relies on the Protection Motivation Theory (PMT), which emphasizes the way people react to threats to information security and how well information security technology works in small businesses (Wu, 2020). Small and medium-sized enterprises (SMEs) in Abu Dhabi emphasis on information security problems, to find workable solutions and research on actions during the conceptualisation process. This study explores perceptions and opinions of SME executives regarding digital adoption and information security (Haydam and Steenkamp, 2020).

The study embraces an interpretivist point of view and uses both qualitative and inductive methods. This study gathers information from 25 participants from SMEs in Abu Dhabi through semi-structured interviews. Among these professionals, 23 are working on management positions while two are serving as officers. Thus, this study is likely to provide expert- -level insights on the impact of digital adoption influenced by COVID-19 effects on the digital adoption at SMEs in Abu Dhabi's context.

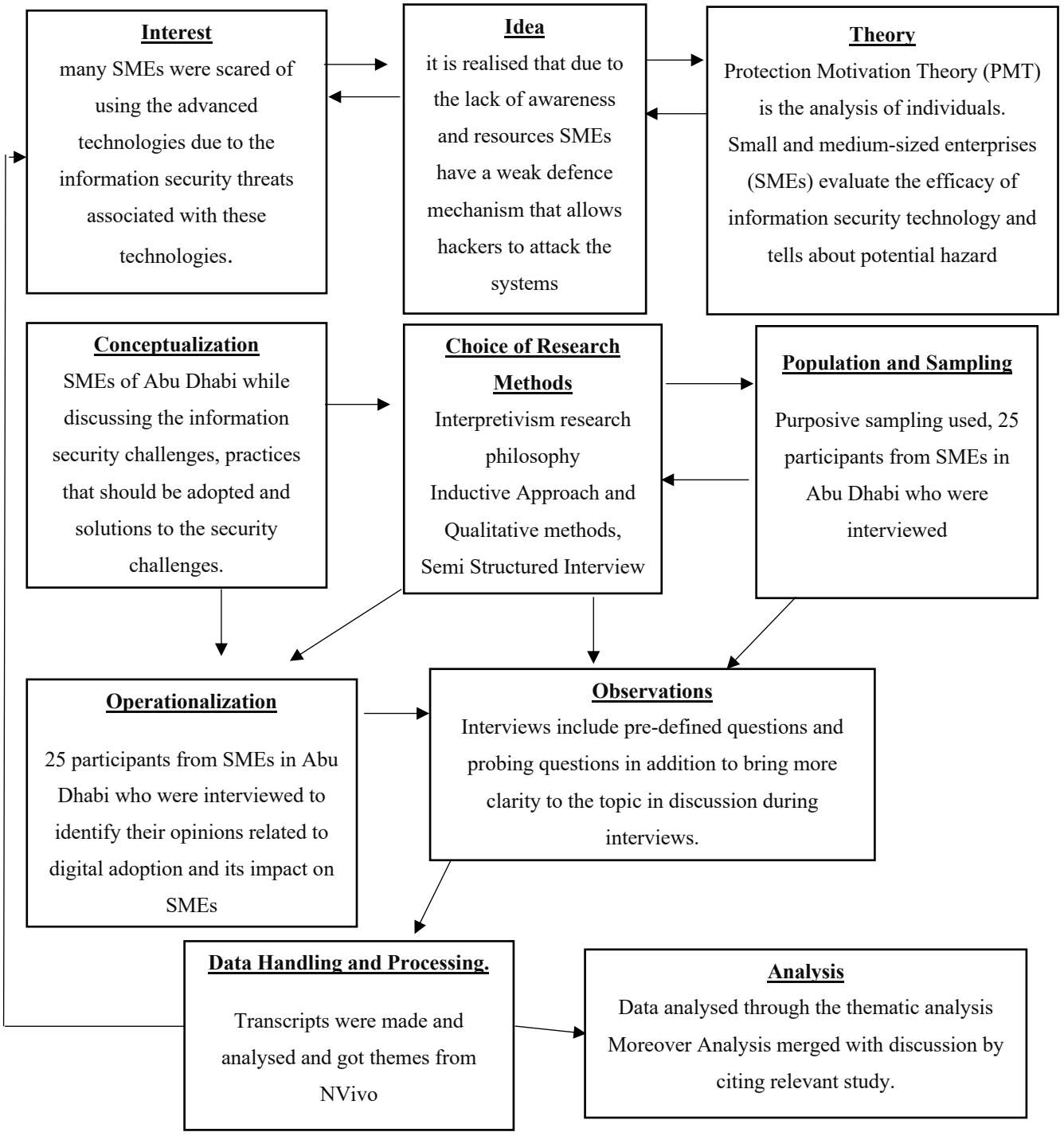

Figure 1-2 Flow Diagram representing the Study, Source: (Babbie, 2013)

According to this sampling method, there is a need to interact with people before choosing the subjects. This plan explained that experts will fully understand the problems that small businesses have when they use digital tools. Recruiting 25 participants (23 managers/leaders and two officers) to discuss

how to use digital technology and how it affects small businesses in Abu Dhabi is a key part of making the plan work. As the process went on, it became clear that the interesting idea turns into a set of facts that can be examined. The researcher asked set questions as well as more in-depth questions during the talks to get rich and useful data. This makes the issues clearer and gives a full picture of how the leaders feel about the problems that come with getting digital.

The researcher used NVivo to make transcripts of the interviews and analyse them. This involves organising and processing the data in a way that makes sense to find themes and trends. Furthermore, the researcher used thematic analysis on the data to find common themes and trends that show how hard it is for small businesses to adopt digital technologies. The analysis is not only a standalone process but is also intricately linked to the initial interest and ideas, providing a comprehensive understanding of the research problem. The analysis findings are seamlessly integrated into the discussion, citing relevant studies and literature, creating a cohesive narrative that aligns with the initial interest and ideas identified. This ensures that the research is not only methodologically robust but also contributes substantively to the existing body of knowledge.

1.9 Dissertation Outline

This study consist of six chapters. This chapter introduces the research problem, determines the research focus, and develops a conceptual framework for conducting the study. The next chapter provides a review of extant literature to locate this study amidst the existing body of knowledge and establish the need for research on COVID-19 related digital adoption on ISM in Abu Dhabi's SMEs. Chapter 3 describes the chosen methods and techniques for research, appropriate for this study. Chapter 4 presents data analysis, depicting thematic analysis for developing research findings. Chapter 5 discusses research findings and compare them with the literary evidence. Chapter 6 includes a conclusion and the recommendations based on the findings of the study.

Outline of Dissertation

Chapter 1 - Introduction

Specifies the direction of the research with clear research problem, focus of the research, and conceptual framework.

Chapter 2 - Literature Review

Effectively presents the importance of the research using comprehensive review of empirical knowledge. It leads to explain the justifcation for the research.

Chapter 3 - Methodology

The chapter outlines the methods, techniques and approaches applied to achieve the answer to research questions.

Chapter 4 - Data Analysis

The focused thematic analysis is provided whcih allows to derive infomartion on the findings achieved from the review.

Chapter 5 - DIscussion

The dicsussion section allows to crticially compare and contrast the research findigns with literature to provide a better overview of the research findings.

Chapter 6 - Conclusion and Recommendations

Provides the summary of the findings and furhter provide evidence of policy and practice based recommendations.

Figure 1-3: Dissertation Outline

1.10 Chapter Summary

The chapter has focused on highlighting the purpose, significance and contribution of the study which is to explore the current situation of SMEs regarding the information security practices and cybersecurity challenges in Abu Dhabi. As the pandemic COVID-19 hit the world, SMEs in Abu Dhabi transformed digitally to continue their business operations. Nevertheless, due to a lack of awareness and shortage of resources, SMEs have weak defence mechanisms providing an opportunity for hackers to detect loopholes and commence cyberattacks. The current study critically evaluates SME cybersecurity and ISM strategies and practices to offer recommendations for policies and best practices of information security for SMEs in Abu Dhabi. The next chapter presents the literature review elaborating on empirical and theoretical perspectives of previous scholars. The gaps in the literature help state the purpose of the following research.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

The advancement of technologies and the use of the internet in different sectors such as banking, education, medical, and others have increased the vulnerability of information to cyber threats. This indicates that as technologies are advancing, hackers can determine cracks and vulnerabilities in information security systems to gain access to sensitive data (Garg, et al., 2018). Cybersecurity measures are significant to limit the exposure of information and data to potential threats. This chapter reviews recent and relevant literature on cybersecurity, its definitions, its fundamentals, models and strategies, theories, challenges, and related aspects of the SMEs operating in the UAE facing increased cyber threats after going digital due to COVID-19.

The literature review did not have a random search strategy, but a systematic search strategy was used to make sure that the results were relevant and high-quality sources in line with the objectives of the study. Key academic databases such as Scopus, Web of Science, ScienceDirect, and Google Scholar were searched with the support of professional and policy reports of the UAE Cyber Security Council, OECD, and the Abu Dhabi Digital Authority (ADDA). Combination of the keywords (SMEs, information security management, cyber resilience, digital adoption, Protection Motivation Theory) were used in the search.

The inclusion criteria were as follows: (1) the source had to be a peer-reviewed or authoritative institutional report, (2) the source had to be published between 2015 and 2024 to be relevant in current times, and (3) the source had to focus on the topic of cybersecurity, ISM, or digital resiliency in SME or organisational settings. The exclusion criteria excluded non-academic opinion pieces, older studies older than 2015 and those that were not related to the SME-scale settings.

The sources were considered in terms of relevance, methodological rigour and theoretical contribution in accordance with the advice of Tranfield et al. (2003). The systematic treatment of the empirical and conceptual works was used as the basis of balanced coverage, which created a strong basis of research gaps and explained the theoretical choice of the Protection Motivation Theory (PMT) and Digital Resilience Theory (DRT).

2.2 Cybersecurity

Azizi and Haass (2023, pp. 22) present a definition of cybersecurity by referring to the NISTIR 7298 report (Glossary of Key Information Security Terms), “Cybersecurity is a concept that involves measures used to protect confidentiality, integrity, and availability of system, and data (such as software, hardware, network), and information being processed, stored, and communicated.” Sciborek et al. (2015) proposed

that information security is part of cybersecurity and that security should be a condition of safety, peace, and no dangers. Wrona (2015) argued that security should be a continuous activity since companies change quickly and need intervention. Thus, cybersecurity is an ongoing effort for businesses to ensure safety (Chalubinska-Jentkiewicz, et al., 2022). Successful cyber and information security requires numerous levels, according to Ekanayake et al. (2020). The report also recommends including people, technology, process, and every component to secure information and data.

Cybersecurity comprises several methods, such as establishing a strong password, managing access to data and systems, upgrading programmes, setting up a firewall, and monitoring for instructions (Smith, 2019). Mamonov and Benbunan-Fich (2018) support this view, highlighting that passwords are the most susceptible cybersecurity element. Hackers may simply access the system if they know user passwords or the system itself. When used appropriately, passwords are a simple and efficient way to protect data, IT infrastructure, and associated systems against unauthorised access (Carstens et al., 2004). According to Tsohou et al. (2015), many employees and homeowners misuse passwords, putting them at danger of online attacks. Smith (2019) emphasises the need of strong passwords. Wash et al. (2016) noted that location names, usernames, person names, single dictionary terms, pet names, family member names, preferred sports teams, number sequences, and so on are readily broken passwords. Strengthening passwords need eight characters. It must also feature numbers, symbols, and lower- and upper-case characters (Peltier, 2016).

Whitman and Mattord (2021) present data and system access control as the authorisation method, supporting Smith (2019). They stress that the management and cybersecurity team must decide who has system access and how much. Lowry and Moody (2015) provide an example of data and system access control. Nieles, Dempsey, and Pillitteri (2017) examined data access constraints in information security standards. They believe information system users should have data access restrictions and that job roles should determine data access. Employees with more responsibilities may access more data than those who require just a limited set to do their jobs. Peltier (2016) explains that user IDs and information system architecture must limit access to essential data to non-unauthorised users. Without control over data and information system access, data and the system are at danger (Peltier, 2016). Qiu et al. (2020) claims that important data is susceptible if all department and hierarchy personnel have access.

According to Humphreys (2008), workers should have access to data depending on their function and the knowledge they require to do their jobs. Zhang et al. (2018) supported Humphrey's claim, noting that marketing workers must have access to consumer insights, market research reports, sales trends, etc. Additionally, Alsharif, Mishra, and Alshehri (2022) opines that the accounting department must have access to accounting transactions and that most other workers should not have access to their work information which accounting and payroll professionals should. Following Baker and Wallace (2007),

an organisation may hold a variety of information types, some of which may be sensitive or vital, and access must be on a need-to-know or a need-to-have basis. This includes financial, personnel, trade secret, research, development, and customer data (Sattarova Feruza and Kim, 2007).

Moreover, Smith (2019) stressed that upgrading programmes is crucial for cybersecurity. Alhayani et al. (2021) expanded Smith's remark by calling software and application updates patches or service packs. Chen et al. (2015) suggested that updates fix security gaps in programmes, apps, and systems. Hongjun et al. (2014) supported Chen et al.'s claim about system loopholes by arguing that an information system's early stages are imperfect, and as data accumulates, imperfections become apparent that require upgrade. Sattarova Feruza and Kim (2007) also noted that the system is designed and tested in isolation and actual work situations are different, therefore, defects and mistakes are possible and must be rectified. Updates improve the system over time and make it tougher for hackers to infiltrate it with dangerous code.

According to Whitman and Mattord (2021), programmes include flaws that hackers may use to get unauthorised access. Updates are crucial to Cybersecurity. Peltier (2016) emphasised that no system or programme is perfect, emphasising the need for constant upgrades. Wang (2005) agreed with Peltier that any system has code defects, no matter how well it is built or developed, and the key to exploiting them is to find them before criminals and immoral individuals. The original programmers constantly seek for issues and repair them. Humphreys (2008) claimed that no system is flawless, and that faults and defects might render cyber defence susceptible. Constant updates find and fix issues to keep the system safe and faultless. Zhang et al. (2010) stressed that cyber threats are growing exponentially. Alsharif, Mishra, and Alshehri (2022) also claimed that cyberattacks, viruses, and complex hacking software are appearing online. Thus, cybersecurity must monitor updates and upgrade gear and software often. Wang (2005) claimed that information security is a risk management strategy that reduces threat impact and occurrence likelihood. Cybercrime prevention includes continuous programme updates to strengthen it (Zhang et al., 2018).

Finally, Smith (2019) recommends installing firewalls to safeguard the network, while Shin et al. (2016) state that firewalls are one of the most established but still critical security solutions for both residential and commercial networks. Firewalls monitor traffic across networks (Alhayani et al., 2021; Alkhudhayr, 2019). Firewall visibility and traffic filtering can detect and block much harmful activity before it reaches the network boundary (Shin et al., 2016). This provides protection in depth, a Merkow and Breithaupt (2014) notion.

Powerful, feature-rich firewalls may compare incoming data to complex rules to protect contemporary networks from a wide range of threats and hostile actions. Traffic should not pass via the device to maintain full communication process security (Chen et al., 2015). Based on their history,

firewalls are categorised into three groups (Li et al., 2019). First and easiest is packet filtering. Packet filtering firewalls govern data flow to and from a network, according to Oppliger (1997). This security feature manages packet flow on the network based on rules, protocols, Internet Protocol (IP) addresses, and ports (Oppliger, 1997).

According to Cheswick (2003), a network packet is a small bit of data sent via networks utilising TCP/IP protocols. Ethernet packets are 1.5 KB, but IP payloads are 64 KB. Several rules determine what communication is permitted and what is not; the former is routed to the other network, and the latter is rejected. Rules include service ports and source/destination addresses. The decision is based on the current packet without connection context (Alkhudhayr et al., 2019). Sun (2015) asserts that this general approach allows the firewall to manage a high quality of service without specific knowledge and incorporate newly generated services it is unaware of. Basic packet filtering firewalls function with junction points like switches and routers, according to Chen et al. (2015). These rudimentary firewalls evaluate packets against the standard, not route them. Sciborek et al. (2015) identified these standards and said that they may be legitimate IP addresses, port numbers, packet type, protocol headers, etc. These firewalls abruptly deleted flagged packets that might cause network problems. Sun (2015) claims that a firewall can handle high-level services without a corporate specialist.

Li et al. (2019) classify firewalls as basic packet filtering, stateful filters, and proxy servers. The authors further classify stateful filters as the second type because they keep connection context beyond packet filters. Li et al. (2019) second type, stateful firewalls, examine packet headers like User Datagram Protocol (UDP), Internet Protocol (IP), and Transmission Control Protocol (TCP)-like packet filtering firewalls. According to Sciborek et al. (2015), stateful firewalls can monitor all connection states and TCP and UDP connections, making them smarter. If stateful firewall clients create a new connection to interact with web servers outside, the firewall generates inbound filters to permit relevant reply to packets from the web server to the clients (Shin et al., 2016). TCP sequence numbers may be used by the stateful firewall to monitor all network connections crossing its border (Oppliger, 1997). According to Li et al. (2019), stateful filters may utilise previously viewed packets while making choices regarding the current packet. Due to the stateful filter's smarter work, the firewall can ensure that certain packet types are protocol-compatible, taking into account message format and communication process position (Oppliger, 1997). However, this requires more memory.

Table 2-1: Sources discussed in the text and their link with each of the devised objectives

Objective	Linked sources discussed in the text
To critically evaluate the information security practices in SMEs in the wake of the COVID-19 pandemic in Abu Dhabi.	Pu et al. (2021); Younies and Na (2020); Cheung et al. (2021); ADC (2019); Bai et al. (2020)
To conceptualise the information security challenges in SMEs in the wake of the COVID-19 pandemic in Abu Dhabi.	Priyono et al. (2020); Ikmal et al. (2020); Mantha and de Soto (2019); Malecki, (2020)
To identify and evaluate the tools and solutions addressing the information security challenges while adopting COVID-19 related digital practices.	Radu, (2018); Murphy (2020); Guven (2018); Costa and Castro (2021); (Maher, 2022; Al-Sharji, et al., 2021)
To critique options for addressing the SME cyber challenges with the development of an associated model for best practice.	Priyono et al. (2020); Papadopoulos et al. (2020); Arroyabe and Arroyabe (2021)

Source: Self-made

2.3 Cybersecurity Issues

There are various kinds of threats that can hinder the state of peace and security of information systems in an organisational setting (Farouk, 2017). Farouk (2015) and Elmrabit et al. (2015) have provided an example in support of Farouk's work- insider threat -by stating that when an employee or a person close to the company gains authorised access to the computer networks. Insider threat, according to Niemimaa (2024) occurs due to careless employee behaviour who failed to make compliance with the business policies and standard operating procedures. For instance, an employee might email critical customer data to a third party (LeFebvre, 2012). Such insider threat mostly occur through human error and it is sometimes intentional. In this regard, insider threat becomes critical. Employees can also click on phishing emails which might provide access to the hackers who want to get into the system. Furthermore, employees might share their credentials with other people who could utilise the access for illegal and unethical means (Burrell et al., 2023).

Similarly, Narayanan et al. (2018) stated that drive-by-download attacks are another kind of threat to information system security such as when a user downloads anything that malicious viruses are installed in the system without permission of users (Narayanan et al., 2018). Malicious code is downloaded from a website via a browser, app, or integrated operating system in a drive-by download

attack without the user's knowledge or consent. According to Rosencrane, (2022), the download may be started without the user clicking on anything. A download might begin even just by entering or viewing a website according to Rosencrane, (2022), drive-by downloads are a common method used by cybercriminals to infect endpoints with exploit kits, other malware, and banking Trojans as well as to steal and acquire personal information (Rosencrane, 2022). These drive-by download viruses can be used by criminals to inject Trojans that collect and steal information from the company and introduce other sort of endpoints and malware (Rehman, Hazarika and Chetia, 2011).

Further, some phishing tricks include tricking users to break security walls. (Berghel, 2012). Grassegger and Nedbal (2021) emphasised that social engineering techniques are used in phishing attacks to persuade users to violate standard security procedures and divulge private information, including names, addresses, login credentials, credit card numbers, social security numbers, financial information, and personal information. Most of the time, hackers send out phoney emails that appear to be from reliable sources like banking institutions, eBay, PayPal, and even friends and co-workers (Rosencrane, 2022). The findings of Farouk (2017) support Rosencrane (2022) regarding fake emails, stating that these threats or cyberattacks are specially designed to access, modify, change, damage, or destroy the data and information for monetary gains or simply interrupt business transactions.

2.3.1 Social Engineering

Social engineering is considered critical by Aldawood and Skinner (2018) because it is one of the most common ways to conduct criminal acts or online fraud. The practice of tricking someone into disclosing private information is referred to as social engineering (Wiederhold, 2014). To con individuals, social engineers use a specific kind of con game (Bakhshi, 2017). Social engineers are those who purposefully deceive and manipulate others for their gain (Alsharif, Mishra and Alshehri, 2022). Huseynov and Ozdenizci Kose (2024, pp. 1) define social engineering as, “In information security context, social engineering is defined as malicious activities caused by cybercriminals by means of human interactions. It is mainly a psychological manipulation technique which gets benefit of human error to reach private information.” The phrase "social engineering" is frequently used in computer systems or the data they hold. Social engineering is the process of utilising deceit or persuasion to get products or information fraudulently. Notably, a victim's emotional condition may have an impact on their readiness to divulge personal information, as discussed by Burov et al. (2020).

Social engineering assaults can target either individuals or corporations. A variety of strategies are used by social engineers to negatively affect targets, including obtaining personal information through deceit, committing fraud, or gaining computer access (Montañez, Golob and Xu, 2020). A social engineering assault has other objectives in addition to gaining access to or control of an information

system. Gaining money or other important goods, such as financial records, may be one of your other objectives. The success of a social engineer is heavily dependent on his or her capacity to build a rapport of trust with the target (Astakhova and Medvedev, 2021). Attacks using social engineering happens on both a physical and mental level, claims Bakhshi (2017). The workplace, phones, trash cans, and the Internet are among the most popular places for social engineers to look for illegal information, get access, and plan psychological attacks. Persuasion, mimicry, obsequiousness, compliance, and friendliness are the main targets of psychological attacks (Wiederhold, 2014).

Human users' propensity to be helpful, their psychological frailties, and their propensity to be oblivious to the importance of the knowledge they hold make them ideal targets for social engineering attacks (Wang, Zhu and Sun, 2021). Social engineering is a collection of tactics used to trick victims into disclosing private information or taking security-compromising activities in the context of information systems security (Mamedova et al., 2019). Attackers who use social engineering frequently prey on people's cognitive prejudices. Social engineering intrusions are human interactions-based, non-technical intrusions that may get past technology security measures. Abass (2018) has described the social engineering attacks by saying that as long as civilization has existed, people have been deceived into giving up money, property, or knowledge.

It is recently shown in different works that social engineering on human psychology and not on technical vulnerabilities. Astakhova and Medvedev (2021) insist that the success of social engineers in their performance depends basically on developed rapport and gained trust with the target, which they use in manipulating human feelings and cognitive biases against malicious ends. This psychological manipulation is a core strategy, targeting human inclinations to trust and help others, which are typically considered positive traits but are exploited in these attacks (Wang, Zhu, and Sun, 2021).

Social engineering methods vary and include activities like phishing, pretexting, baiting, and scare ware (Azhar et al., 2023). Attacks come into play through the manipulation of human feelings that vary between fear and curiosity. For example, hackers may try to instil fear through the use of urgency and authority. They would force individuals to act in undue haste with less scrutiny. Else, they may apply the effect of exposure wherein familiarity breeds complacency, which may easily make one trust unlawful communications or links that are valid in appearance.

Burda, Allodi and Zannone, (2024) argue that cognitive biases act as a critical enabler regarding the commitment of social engineering attacks. Cognitive biases, including confirmation bias, anchoring, and choice-supporting bias, amongst others, are those pains-in-the-throat that distortedly affect rational thinking and make an individual exposed to their use susceptible to manipulation. For example, social engineers create situations that reinforce entrenched beliefs or that leverage first impressions, anchoring

their fraudulent deal within what seems like a credible context; this can include emulating the visual and textual cues of trusted entities.

The workplace and online environments are high-target platforms where social engineering can occur with relative efficiency because of the intense number of personal and professional exchanges. Many attackers build information from publicly available sources such as social media or company websites to construct plausible deceptions (Teasley, 2023). The increasing sophistication of these attacks is often linked to the rich data environment of digital platforms, where users frequently share and access personal information.

The complexity and increasing prevalence of social engineering attacks raise the demand for a comprehensive security education and awareness training programme. A proper security culture of critical thinking and suspicion should be engrained into the employees, especially when receiving unsolicited requests for information or access. According to Klimburg-Witjes and Wentland (2021), good training would increase the ability of employees to have more knowledge about various kinds of social engineering tactics and methods of psychological manipulation by an attacker.

Kaushalya et al. (2018) have presented the statistics related to social engineering attacks and argued that social engineering attacks have increased with an exponential growth rate. With the advancement in technology, social engineering attacks are likely to increase, as improved cybersecurity measures make them a far better alternative for hackers. Where individuals and policies are most vulnerable, social engineers strike. The four assault vectors of fear, kindness, carelessness, and are how Breda et al. (2017) classify social engineering attacks. Social engineers take use of these emotional states to obtain the knowledge they need. For instance, an attacker may utilise name-dropping or business lingo to get the victim to provide the information they otherwise would not feel comfortable doing (Breda et al., 2017). Alternately, the attacker may pose as a higher-ranking employee and utilise the urgency of the situation to instil dread and a feeling of duty in the victim. Hence, it is important for companies and individuals that they understand social engineering to prevent such attacks. Awareness regarding Social engineering is necessary to create a sense of security in the cyber business world Klimburg-Witjes and Wentland, 2021).

Aldawoods and Skinner's (2018) study, a secondary research, examined numerous studies on the social engineering attack in the online world and concluded that attacks done by social engineering tactics cannot be eliminated because of their unpredicted innovations, but the awareness of social engineering can help mitigate the losses and prevent companies from these threats to information security of companies (Aldawood and Skinner, 2018). In support of Aldawoods and Skinner's (2021) study, Foord and Gulland (2006) stated that human error cannot be eliminated with technology implementation.

Similarly, Mulholland (2018) argued that elements associated with human are quite complex to predict, prevent and detect errors as compared to the computer system and machines. In addition to this, human in the workplace while handling technology perform at different capacity and scale and therefore performance level remains inconsistent. Hence, the risk associated with human error cannot be eliminated (Mulholland, 2018). Human error cannot be eliminated is also supported by Osoba and Welser IV (2017) who stated that even the Artificial Intelligence (AI) system which is capable to do work on its own can be affected by human error. AI Bias is one limitation where humans are involved in developing an AI system but biased frame of mind. In this way, with a highly sophisticated system, human error cannot be eliminated (Osoba and Welser IV, 2017).

Social engineering is a technique or threat against security that works by manipulating human behaviour and associated weaknesses to achieve a malicious purpose (Mouton, et al., 2014). When planning and carrying out their attacks, social engineers depend on cognitive biases or flaws in the mental process to elicit their target's involuntary emotional responses (Corradini, 2020). Rains (2020) maintained that anchoring, exposure effect, and/or decision-supporting bias are examples of cognitive biases. An individual may accidentally input his or her credit card information to a bogus site posing as for instance, eBay, stating they have not received payment on a purchased item, due to choice-supporting bias, which is the propensity to recall earlier events as being better than negative (Ponnusamy, Selvam and Rafique, 2020).

Owing to confirmation bias, people will gather and interpret data in a way that supports their opinions (Hijji and Alam, 2021). For instance, if staff members frequently see caretakers wearing a particular uniform, they might not react with concern when they spot a phoney wearing the same attire. As a result, the social engineer may use the system without having to provide personal information. Given the exposure effect, individuals like things and people that are familiar to them (Mustafa, 2019). For instance, a user of online social networks would be more inclined to visit a malicious website that advertises itself as an 'online dating service.' Anchoring implies that a person concentrates on seeing a distinguishing characteristic (Klimburg-Witjes and Wentland, 2021). Visitors may be duped, for instance, by bogus websites that exhibit identical logos to real banks.

Luo et al. (2011) have conducted a study on the neglected human factor associated with information security. The objective of Lou's study was to study human factors that could affect information security adversely and based on analysis, researchers have identified social engineering as the major tactic which hackers used to infiltrate the system. Based on the inductive approach and involvement of human understanding, the researchers come up with a particular step which hacker uses for social engineering attack. In addition to this, the researchers have identified that entities often fall prey to social engineering

attacks including new employees, clients and customers, IT professionals, and top-level management (Luo et al., 2011).

Similarly, Conteh and Schmick (2016) researched to determine the vulnerabilities in the IT infrastructure of an organisation. The researchers conducted a secondary literature review that has taken those studies that explicitly determines the vulnerabilities in information security systems. The study noted that to overcome the incidents of social engineering attacks, the most common tactic is to hire an educated computer user, this is one of the most supportive and effective defences against social engineering attacks. The research found that the most vulnerable entity to cybersecurity attacks include the new employee in a company. The study concluded f that technology plays an important role in reducing social engineering attacks. The vulnerability exists with psychological predispositions, human impulses, and behaviours that can be impacted through education. The paper suggested that organisational educational campaigns enable users to reduce social engineering attacks. Educational campaigns for overcoming cybersecurity threats are the factors that are yet to be put forward (Conteh and Schmick, 2016). The limitation of the research has been that they did not attempt to expand the solutions that could be used to minimise the threats. Further, the paper did not highlight how frequently training is required for employees regarding social engineering threats. However, Wang et al. (2021) presented an argument criticising the idea of hiring experienced and technical employees in the cybersecurity domain. According to them, to reduce social engineering attacks, the cybersecurity team needs to have a comprehensive training and development programme where experienced employees can train new information security candidates and turn them into an expert. Mouton et al. (2014) hold a similar notion and stated that all experts in the information security domain are not a cost-effective way to manage it. Ghafir et al. (2016) assert that even company hire educated computer user, human error risk will remain, and it can be avoided by taking strict follow-ups and enforcing policies rigidly over the employees. Nguyen and Bhatia (2020) strongly emphasise on training and development programmes, accentuating that such programmes help employees to become more aware of the current situation and makes them more vigilant towards various cyberattacks.

These four steps were discussed by Luo et al., (2011), have been briefly defined below:

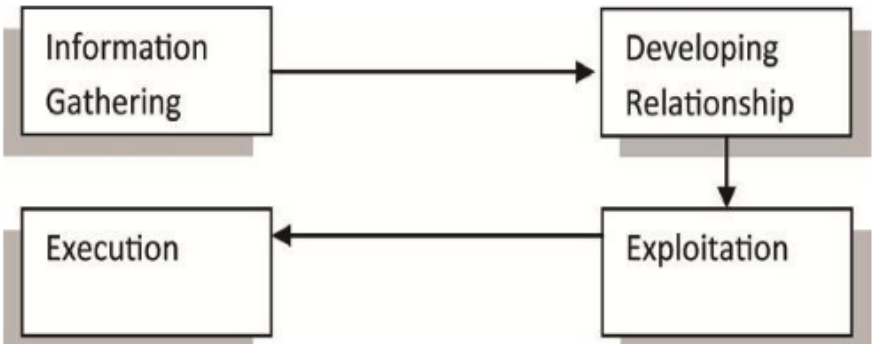

Figure 2-1: Social Engineering Stages, (Source: Luo et al.,2011)

Information gathering: The first stage is where the information on the potential target is gathered extensively (Figure 2-1). The potential of most attacks is dependent on this phase; therefore, it is natural for criminals to spend the majority of their time gathering information about the target (Luo et al., 2011). Mountain et al., (2014) hold similar views and stated that the right information about the target can facilitate attackers to determine the possible password, and attack vector, refine the goal, and likely responses from individuals (Mouton et al., 2014). At this stage, by gathering information about the target, the attacker becomes comfortable and familiar with the person to attack and easily formulates a strong excuse (Asnawi et al., 2020). According to the study conducted by Chitrey, Singh and Singh (2012), around 93% of the respondents claimed that attackers use social media platforms like Facebook, Instagram, or google applications to collect information. However, Krombholz et al., (2015) disagree with the concept and stated that at the initial stage, the attacker check system vulnerabilities first so that he can have an idea of what sort of information he needs to collect.

Relationship building: At the next stage, relationships are established with the target and this stage is considered of high importance for attackers (Medan, 2020). Medan in the study further argued that the level of cooperation will help decide the support attackers can gain from the target in accomplishing his goal of stealing information. Yan and Gao (2007) stated that relationship building is all about developing trust, hackers will be able to begin obtaining the sensitive data and access required to compromise a system after trust has been built (Zulkurnain et al., 2015). A good hacker would gather information over time by soliciting little favours or listening in on discussions that look benign Junger, Montoya and Overink, (2017) argued that trust can be gained by reflecting authority where a person shows himself as a person with authority which influences the employees and users of the system to provide them with the information. Similarly, in support of Yan and Gao's statement, Kumar et al. (2015) stated that the hacker will put a lot of effort into keeping up the appearance of innocence while learning corporate

jargon, the names of significant employees, the names of crucial servers and apps, and several other crucial details (Kumar et al., 2015).

Exploitation: The third stage is the exploitation stage in which the attackers have successfully gained unauthorised access where the attackers use information and relationships for infiltrating the targets (Luo et al., 2011). At this stage, attackers aim to maintain compliance with the momentum that has been created at stage 2 (Clarke and Furnell, 2020). According to Mouton et al. (2014), Social engineering, which is part of the information security spectrum, focuses on using people as tools to obtain unauthorised access to information. Although most organisations focus on people, those people also present risks to those organisations. Similarly, Zulkurnain et al., (2015) stated that employees are the users of the information systems and they can be the most legitimate source of information which hackers want, therefore, there is a higher chance that employees can be exploited for information.

Execution: Finally, in the last stage, which is execution, the hacker implements the attacks to cause damage and misuse the retrieved information where, hackers or attackers successfully achieve their goals (Luo et al., 2011). As per Medan (2020), hackers steal information without letting the victim know that they have been attacked. Moreover, the attackers keep their identities hidden which facilitates further activities (Medan, 2020). Zulkurnain et al. (2015) argued that execution is the stage in which social engineers use what they have learned from the previous phase, therefore it is neither directly about social engineering nor the beginning of a new cycle. However, according to Hadnagy (2010), decisions taken during this latter stage might result in the attack's success. For example, during the execution phase, actions are taken in the fields of hacking and cracking or outright theft rather than social engineering; however, this phase attracts special attention because the success of this phase depends on the success of the social engineering act (Zulkurnain et al., 2015). Actions taken in this phase are more of a technical nature than psychological nature. For example, physically accessing the system and installing malware makes it possible to hack a computer system that cannot be infiltrated through remote networks. (Hadnagy, 2010). Hadnagy further stated that the theft or destruction of a physical object might also be the final goal of the assault, which would involve social engineering to learn where it is and gain access to it (ibid). Any information that is recovered during this phase will depend on the attacker's objectives; however, it may also include all of the infrastructure data for the target company (Jamil et al., 2018). Salahdin and Kaabouch (2019) also supported these four steps involved in social engineering attacks when they surveyed the social engineering attacks. The study of Salahdin and Kaabouch has adopted an inductive research approach and defined that technological advancements have made communication accessible and instant for humans, but technological measures to protect the information still lacking. The information systems are vulnerable and exposed to malicious social engineering attacks, some techniques that can be considered to overcome crimes include anti-virus software systems, intrusion

detection systems, installing pop-up windows regarding virus detection, encouraging social security training for employees, and providing tools to prevent from the attacks (Zhou and Pei, 2008;Sadeghi, Wachsmann and Waidner, 2015). Further, creating an awareness of social attacks, teaching employees the ways of keeping the information confidential, and advertising attack risk to all organisational employees (Salahdin and Kaabouch, 2019). Distinctively, Clarke and Furnell (2020) presented an extended form of steps in the process of social engineering, for example, the first step in the process is attack formulation which includes the activities of identifying goals and target identification (Sadeghi, Wachsmann and Waidner, 2015). However, the last step in the process is debriefed which includes maintenance and transition (Luo et al., 2011).

The social engineering threats are complex as its infrastructure is complicated and the technique involves the exploitation of human vulnerabilities that are challenging to address using automation (Uebelacker and Quiel, 2014). Wilcox and Bhattacharya (2016) determined an increased usage of social media users in the workplace by staff and employees revealing organisational information to threats and vulnerabilities as the layers of cybersecurity became weaker.

The study by Pettit (2022) used a secondary approach to reflect on the types of social engineering attacks such as whaling, phishing attacks, baiting, pretexting and so on. While the study was not specific to any country, it was generally done regardless of any border, most of the data has been taken from the United States' websites. The strength of the paper has been that it highlighted the types of social engineering attacks and proposed recommendations. However, the weakness of the study is its limitation in the explanation of the ways these attacks work. The author called social engineering an elevated form of malicious activity. Handnagy (2019) also supported the same statement and regarded social engineering as malicious activity.

Social engineering achieves its precarious purpose by using five types of attacks Phishing, Baiting, Pretexting, Tailgating, and Quid pro quo (Adu-Gyimah, Asante and Boansi, 2022). Phishing refers to an activity or behaviour of attacking end-users by taking an advantage of human psychological factors or computer technology (Stephanidis and Antona, 2020). According to Molia and Gohel (2015), Phishing is a strategy used in internet communication when a social engineer poses as a reliable person or company to lure victims into providing information and passwords. Molia and Gohel further stated that before becoming common on the Internet, phishing was carried out over the phone, which is why the term "phishing" is used to describe the practice (Molia and Gohel, 2015). According to Gupta et al. (2017), the current method of phishing on the internet involves sending the target an email or pop-up that directs them to a website that looks a lot like a page they are already acquainted with. This page often asks the user to enter their login and password (Gupta et al., 2017).

Chiew et al., (2018) conducted research that stated another phishing method used by social engineers to collect information is mail-out. Mail-out is an attack where a recipient gets the message thinking it is authentic (Handnagy, 2019). A survey delivered to employees of a company, with a reward offered as if it were a lucky draw contest, is an example of a mail-out survey (Chiew et al., 2018). Spyware or Malware can also be propagated through the mail-out strategy, which often involves attaching it to the files that are delivered to the target (Abass, 2018). As a social engineering method, mail-out may also be used to establish targets for reverse social engineering (Adu-Gyimah, Asante and Boansi, 2022).

Baiting is also like phishing attacks, the only difference is, that baiting offers an item or a good to induce victims. For example, baiting asks users to download movies or songs by logging in to their accounts (Lacey, Salmon and Glancy, 2015). Successful social engineering assaults frequently include several various techniques, if not all of them (Adu-Gyimah, Asante and Boansi, 2022). The most potent social engineering tools, nevertheless, were developed using socio-technical methods (Zhou and Pei, 2008). One such is the so-called "baiting attack," in which criminals place malware-infected storage media in a spot where potential victims are likely to discover it (Sadeghi, Wachsmann and Waidner, 2015). For instance, it may be a USB disc with a Trojan horse on it (Narayanan et al., 2018).

Pretexting is also a malicious activity that can be used to attack users (Conteh, 2021). While using the pretexting technique, attackers focus on developing a pretext through which they steal the personal information of people (Whiteman III, 2017). This sort of attack is usually done by reliable and trusted entities, and they ask to confirm confidential information for confirming the identity (Workman, 2008). Hadnagy (2010) stated that Pretexting is the most popular kind of social engineering, which entails fabricating a false situation and exploiting it to convince a potential victim to freely divulge information or do certain actions.

Quid pro quo is another malicious attack that has been designed to steal the information of someone; this is more like baiting (Lacey, Salmon and Glancy, 2015). Quid pro quo refers to giving something in exchange for something else, and in this case, the attacker provides free services in exchange for the target's information (Pettit, 2022). According to Junger, Montoya and Overink (2017), the information was collected with malevolent intent. Attackers typically use phishing to phone random numbers while pretending to be from the technical support team or help desk department of the target service provider (Conteh, 2021). Conteh further stated that they use question-and-answer exercises to alter the target's system to breach it or gain private or secret information. The victim is persuaded by the attacker to input instructions that grant him access to break security or launch malware that opens backdoors on the victim's computer (Krombholz et al., 2015).

Conteh and Schmick (2016) also justified that the victims are attracted and persuaded by the hackers in both phishing and baiting, the only difference is that goods are offered as gifts in baiting whereas

phishing involves deception and misleading users to provide their credentials (Conteh and Schmick, 2016). Similarly, Quid pro quo promises to provide technical service in exchange for personal credentials (Salahdine and Kaabouch, 2019). While pretexting incorporates a fabricated scenario to obtain information, tailgating uses piggybacking to reach the restricted data, often by impersonation or gaining information about authorized accesses (Breda, et al., 2017). Regarding phishing, Kamel (2021) noted that financial phishing has become popular among cyberattackers to steal money from the target. One of the reasons could be that it required small investments and technical knowledge and can propagate rapidly.

A study by Thomas et al. (2017) explored the causes and the mechanism behind social engineering attacks with the help of a team of researchers from Google. The researcher examined the method of data theft that was employed by the attacker to steal numerous credentials and used it for malicious reasons. From all the participants, the study detected 788,000 people who showed vulnerability to off-the-shelf keylogging. Whereas, among the total participants more than 12 million were found to be a target of phishing, and 2 billion credentials were determined that showed that social engineering was used to retrieve these usernames and passwords. The findings of the study by Thomas et al., (2017) produced implications to train and prepare staff and employees against social engineering and other types of attacks such as malicious content, phishing, trojans, etc.

2.3.2 Malware Attacks

Various cybersecurity professionals and experts suggest that malware is among the most prevalent choice of cyber threats to conduct malicious acts and breach security (Siponen and Oinas-Kukkonen, 2007). Jang-Jaccard and Nepal (2014) declared that malware includes a variety of attacks that are commenced on the system silently to steal information, cause damage, or manipulate the system. Some of the malware includes viruses, trojan horses, worms, spyware, and others like bot executables (Jang-Jaccard and Nepal, 2014). Passeri (2016) provided the case of various cyberattacks and their percentages of occurrence in 2016. Malware (35%) was the most conducted cyberattack in 2016 followed by Distributed Denial of Service (DDoS) (15%), targeted attacks (10%), and others as shown in Figure 2-2. The future of malware was discussed by Bakdash et al. (2018), using seven years of data on cyberattacks, the study developed cyber even forecasting to predict the malware attack or cyber event a week before like weather forecasting. In 2020, 78% of the total SMEs in the UAE reported that they were attacked by malware attacks, especially ransomware, and disruptions due to this cyber threat were found to be increased by 66% (Sadaqat, 2021).

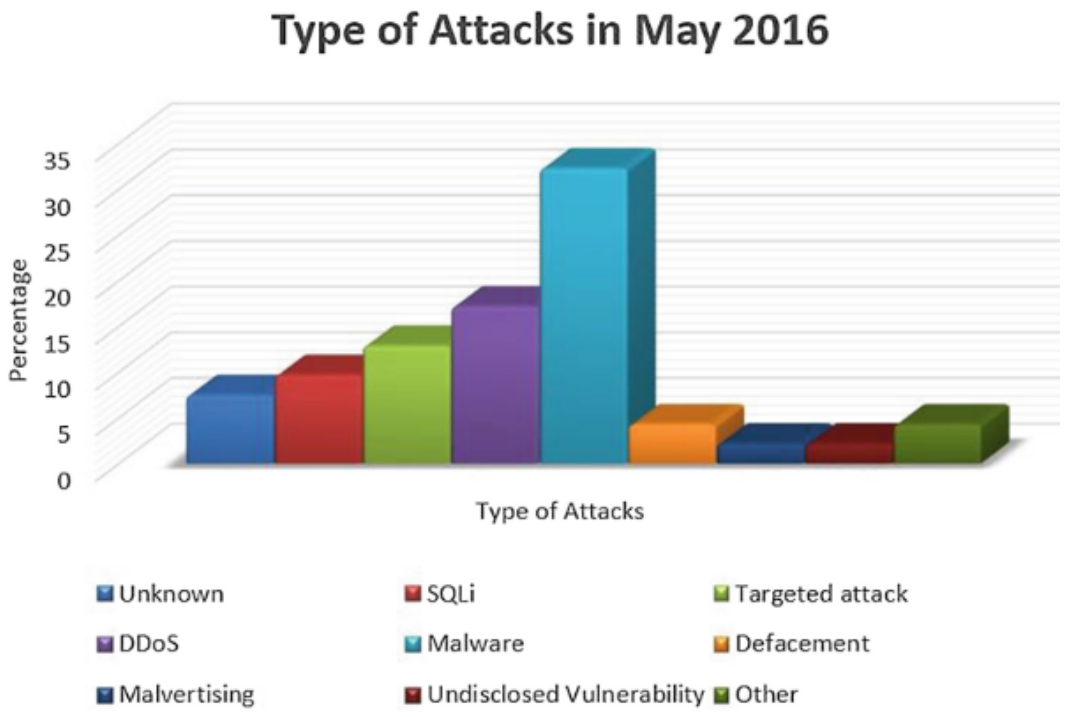

Figure 2-2: Attacks in 2016 worldwide Source: Passeri (2016)

2.3.3 DDoS and DoS

DDoS and DoS are different sorts of attacks that are designed to overwhelm the sources of a system to the where they are unable to reply to the requested services such as Denial of Service (DoS) (Peng, Leckie and Ramamohanarao, 2007). Similarly, Peng, Leckie and Ramamohanarao also find ways to drain the resources of a system. In Distributed Denial of Service (DDoS), the attacker control and vast array of malware-infected machines (Zargar, Joshi and Tipper, 2013). According to Maslan (2018), these attacks are also known as "Denial of service" acts because the targeted site is unable to deliver the services to the users who used to access them.

DDoS works in a way that all sites are flooded with illegitimate requests, and the website has to respond to each request (Balarezo et al., 2021). In this scenario, the site is unable to answer the queries of visitors as it normally does lead the site towards complete closure (Zhang and Green, 2015). DDoS enables hackers to gain an access to the site or enhance that access so the hackers can benefit from their activity (Galeano-Brajones et al., 2020). The objective of this attack is to influence the effectiveness of the target's activities (Douligeris and Mitrokotsa, 2004).

Some internet hacking is attributed to market competitiveness. According to Galeano-Brajones et al. (2020), competition might cause organisations to take extreme steps to avoid competitors. Hacking to disrupt the rival company's operations or hurt its finances has been found by researchers (Zargar, Joshi and Tipper, 2013). Hackers are rewarded well if the competition is engaged (Modi et al., 2013).

Yan et al. (2015) noted that cloud computing's critical properties are boosting DDoS assaults, while software-defined networking may lessen them. “Software-Defined Networking (SDN) is an approach to networking that uses software-based controllers or Application Programming Interface (APIs) to communicate with underlying hardware infrastructure and direct network traffic” (Vmware, 2022, p1). New SDN capabilities may resist DDoS assaults and decrease service disruptions (Peng, Leckie and Ramamohanarao, 2007). SDN allows centralised network management, software-based traffic monitoring, dynamic forwarding rule updating, a global networking perspective, and DDoS detection and response (Behal and Kumar, 2017). DDoS assaults have always raised security concerns (Dong, Abbas and Jain, 2019). Despite several advantages, Zkik, El Hajji, and Orhanou (2019) claimed that implementing SDN requires changing the whole infrastructure, making it expensive. Zkik, El Hajji, and Orhanou (ibid) also suggested that SDN requires new management tools and training for everyone. Lee et al. (2008) state that SDN lacks security requirements and that third-party service providers do not solve security challenges. Only experienced SDN managers can stop major dangers.

2.4 Targeted Attacks

Targeted attacks refer to malicious activity that aims to disrupt normal network’ operations (Sharevski, 2018). Sharevski, (2018) argued that normal network operations mean that system is managing data and different transaction request in a normal manner and with standard speed and accuracy. In a targeted assault where the main objective is to disrupt normal network operations, threat actors deliberately seek out and breach the infrastructure of a target organisation while remaining anonymous (Gezer et al. 2019). These attackers possess the knowledge and resources necessary to carry out their plans over an extended period. Jahankhani (2017) defined targeted attacks as a type of threat that is carried out with a range of threats which include affecting command and control communications, lateral movement, point of entry and so on (Gezer et al. 2019). Targeted attacks are illegal attacks by criminals that are done with long-term planning of attacking the victim (Korba, Nafaa and Salim, 2013).

In more simple words, targeted attacks specify the victims and contain long-term endurance (Gezer et al. 2019). Further characterisation can be done by the attackers’ capabilities and dedication to deploying the attack (IBP Inc., 2013). Targeted attacks pose a significant threat to commercial and government entities; with the years an increasing number of threats are being observed and multiple cybersecurity organisations are facing the issue of targeted threats. The major characteristic of these attacks is that they are conducted by skilled and educated people (Jawandhiya et al., 2010). Targeted attacks use sophisticated tactics and tools such as zero-day or software exploits, watering hole techniques, and customized spear-phishing emails to gain a lasting presence in the breaching environment (Giuffrida, Bardin and Blanc, 2018).

2.4.1 Viruses, Worms, Trojans

According to Kamel (2021), business users were the main target of more than 38% of the total 25,811 malware attacks which consisted of viruses, worms, and trojan horses with the purpose of financial attack whilst Hughes and DeLone (2007) differentiate between the viruses, worms and Trojan.

- Viruses are executed via executable files (Hughes and DeLone, 2007).
- Trojans execute through a programme which is dubbed utility software (Hughes and DeLone, 2007).
- Worms are executed via weaknesses in the system (Hughes and DeLone, 2007).

A computer programme or software that connects to another programme or computer to destroy a computer system is known as a virus (Tohme et al., 2015). When a virus-infected computer application is started, it does certain actions, such as removing a file from the computer system (Hughes and DeLone, 2007).

While worms are a type of computer software like viruses, they do not alter the programme (George, 2015). It keeps reproducing itself, slowing down the computer system (Barret, 2015). Unlike viruses and worms, the trojan horse does not replicate itself (Gezer et al. 2019). According to Kuzmenko (2020), it is a covert piece of code that steals the user's vital information. The e-mail ID and password, for instance, are observed by Trojan horse software when entered into a web browser for logging (Kuzmenko, 2020).

In 2010, the Stuxnet worm (name derived from a keyword combination in software) become prominent in the second half crashing industrially controlled computing devices in various economics in the MENA region. The Stuxnet infection was created specifically to target an Iranian nuclear processing plant at Natanz (Wolf, 2010). Stuxnet especially targeted Personal Computer (PCs) that run the Siemens SIMATIC Step 7 industrial control programme (Wolf, 2010). It attacked Windows computers and employed well-known tactics to steal data and disguise itself from a victim's PC. The SIMATIC control programme was widely used in the industrial sector which is why it was a great cybersecurity threat to the MENA region (Ibid).

The study by George (2015) focused on Stuxnet attacks and the impacts of cyber worms, explaining how it turns off lights, disables cameras, manipulates drones to land in the danger zone, etc. Concerning this, Barret (2015) discussed the attack of Stuxnet and stated it was the product of increased reliance on technological practices. Aligning with this notion, the situation in UAE became vulnerable after COVID-19 as businesses adopted digital technologies and hackers exploited the information security vulnerability in the SMEs (Check Point Research, 2022). Companies that have transitioned towards remote working are at greater risk because under remote working, management faces the challenges to supervise employees' activities (Ibid).

According to the report of Kaspersky Lab (2015) mentioned the trends of cyberattacks in the UAE, it was demonstrated that mobile-based financial attacks were the top-most malicious content to steal money (Kaspersky Lab, 2015). The report explained that baking trojans, two families of them were determined to be among these top-most threats in 2015 such as Fake-token and Marcher, respectively (Kaspersky Lab, 2015). On the contrary, a global analysis of the trojans by Check Point Research (2020) named Ramnit and Trickbot as the prevalent banking trojans in the finance and banking sector globally. The TrickBot virus was first introduced as a Trojan horse in 2016 and has since developed into a modular, multi-phase malware that can do a broad range of illegal activities, such as: stealing a resume (Gezer et al. 2019). Another banking Trojan used to identify files that execute viruses that propagate via portable devices and steal private information, including stored File Transfer Protocol (FTP) passwords and browser cookies, is called Ramnit (Kuzmenko, 2020). Ursnif attempts to steal banking and online account passwords while stealing system information. Removal. Automatic response; suspect an improper file detection.

The banking Trojan known as DanaBot originally targeted Australian customers with emails that contained phishing URLs. Then, as part of a series of extensive attacks, criminals created a second variation and targeted US corporations (Montalbano, 2021). Montalbano further discussed Dridex and stated that the Trojan-like Dridex virus cloaks its dangerous coding in seemingly benign data. Dridex malware's primary objective is to steal private information from its victims' bank accounts, such as their login information for online banking and financial access (Black and Opacki, 2016). Another common Trojan in the banking sector is called QBot (Ibid). It is often distributed through phishing tactics to persuade users to accept malicious files or to trick them into visiting counterfeit websites that employ vulnerabilities to run QBot on the victim's computer (Black and Opacki, 2016). Figure 2-3 shows a global distribution of prevalent banking trojans indicating that 32% were Trickbot, 19% Ramnit, then comes Ursnif, then DanaBot (6%), Dridex (6%), QBot (3%), and others (26%). The report is based on the insights from the previous year 2019 regarding major cyberattacks and generated predictions for 2020.

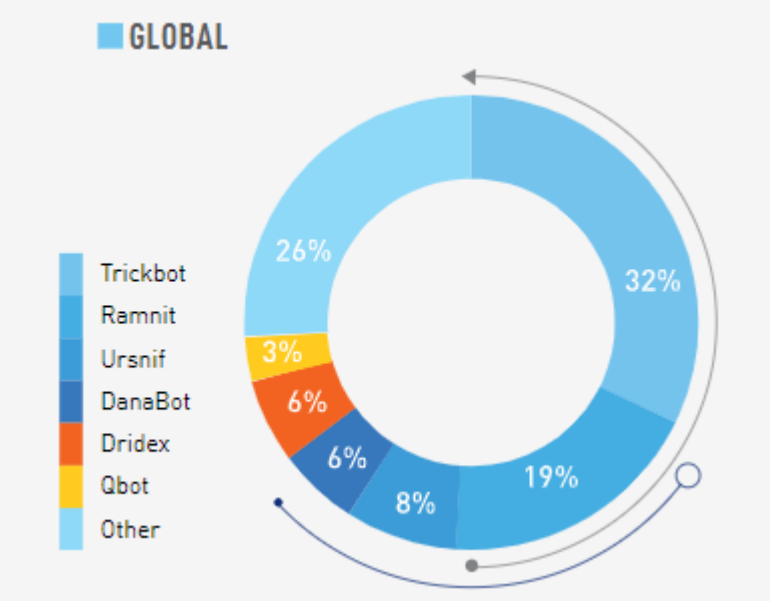

Figure 2-3: Cyber Attack, Source: (Check Point Software Technologies, 2019)

Furthermore, the overall picture of computers in the UAE affected by viruses trojans, and worms is not desirable (Younies and Na, 2020). Tohme et al. (2015) mentioned that the total number of computing devices in the Middle Eastern region infected by viruses is greater compared to the global average. Tohme et al, (2015) further argued that the reason behind such a high number is the lack of awareness regarding cybersecurity among mobile and Pcs users. Such lack of awareness leads to vulnerable organisations in the cybersecurity field as well. In addition to this, Check Point Research's (2022) results further affirmed the statement of Younies and Na (2020) that the UAE situation related to cybersecurity is not desirable.

According to Check Point Research (2022), cyberattacks in the UAE increased by 71% and 50% globally. In 2021, the education sector experienced the highest volume of attacks, with an average of 1,605 attacks per organisation every week which is 75% more as compared to 2020. This was followed by the government/military sector, which had 1,136 attacks per week which are around 47% more as compared to 2020. Similarly, the communications industry had 1,079 attacks weekly per organisation which is 51% more as compared to 2020 (Check Point Research, 2022). Check point report highlighted that hackers are innovating their procedures due to which they are finding ways to trespass the existing cybersecurity layers.

2.4.2 Ransomware

Ransomware is another type of malware attack that has emerged recently as a threat to information systems leading to financial loss and data theft (Gazet, 2010). Kesaya 2021 was affected by Ransomware where the attackers demanded 70 million USD in the shape of cryptocurrencies (Dossett, 2021).

Similarly, JBS Inc. which is considered the largest meat supplier was affected by the ransomware and the company paid 11 million USD to the hacker to protect the data (Collier, 2021). Hampton and Baig (2015) stated that ransomware uses malware injection and hides in the end-user device followed by demands of extortion of information or system credentials, this malware attack required immediate attention. Ransomware is called a global nightmare in 2015 it was observed that in one in every six (17%) ransomware threats, an android device is involved (Kaspersky Lab, 2015).

The trends of 2015 showed that there is an increase of more than 180,000 users attacked by encryption ransomware, and the figures have increased by 48.3% compared to the previous year (Kaspersky Lab, 2015). It is mentioned that server attacks and ransomware (18%) were among the top threats across the Middle Eastern Region, only misconfiguration was found to be closer (14%). These ransomware attacks are implemented by malicious agents, Jasper (2015) mentioned that malicious agents can be terrorists, state-organised hackers, foreign powers, hacktivists, data thieves, nation-states, etc (O'Kane, Sezer and Carlin, 2018). The study by Murphy (2020) stated that malicious agents demand ransoms from governmental agencies and healthcare companies when they successfully conduct a ransomware attack. System downtime was faced by the businesses due to ransomware attacks, companies lost about 6 days of work, and about 29% of UAE businesses stated the downtime continued for a week or so (Sadaqat, 2021). In the same study, 43% of the victims facing ransomware attacks stated that they gave the ransom money to the hacker but only about 44% obtained their data; more than 56% of people did not get their data back even after paying the ransom (Sadaqat, 2021).

According to Silva et al. (2019) ransomware attacks in the past years have grown by 46% such that several different variations have been included. The attackers have become sophisticated as they are exploiting novel infrastructures like IoT, police departments, hospitals, and government agencies among others (Azmoodeh, et al., 2017). Among the new variants of ransomware, GandCrab emerged in the middle of the year 2018, with further progressive variants like Nemucod, CryptorBit, Chimera, Jigsaw, and so on were added to the list (ESET, 2018). GandCrab ransomware is a kind of malware that encrypts victims' files and demands a ransom payment to restore access to their data. It was first discovered in January 2018 (Usharani et al. 2021). GandCrab targets organisations and individuals that use Microsoft Windows-powered PCs (Lemmou and Souidi, 2018). But throughout most of its brief but deadly existence, GandCrab generally propagated via a programme known as an exploit kit (Ibid). Exploits are a type of cyberattack that use a target system's flaws or vulnerabilities to provide unauthorised access to that system (Ibid). An exploit kit is a plug-and-play collection of diverse technologies created to exploit one or more vulnerabilities (Lemmou and Souidi, 2018).

A Ransomware called Nemucod distributes further malware onto the machines of its victims. This programme is spread by online criminals through emails with associated zipped files (Broadhurst and

Trivedi, 2020). These emails frequently make the pretence of being official invoices, court summonses, or other papers (Ibid). According to Symantec, Nemucod was originally identified in December 2015 and was linked to downloading malware, such as a ransomware version called TeslaCrypt. Workstations of users are infected by the malware TeslaCrypt using several attack kits (Craciun, Mogage and Simion, 2018).

A ransomware tool is known as CryptorBit that targets all Windows versions was launched at the start of December 2013 (Alzahrani et al., 2020). CryptorBit attacks computers by tricking users into installing the virus by disguising it as a legitimate antivirus programme or an update for well-known software programmes like Adobe Flash (Ibid). After the files have been encrypted by CryptorBit, the user is prompted to install the Tor Browser, input their email, and continue the on-screen directions to deposit the extortion money (Naseer et al., 2020).

The Chimera ransomware has been around for a while, and although it was thought that the operation had ended in 2015, it has just returned with an update that is much more dangerous than before (De Oliveira and Sassi, 2020). As a Trojan, Chimera depends on its victims to share and install the software to propagate because it is unable to do it on its own (Islam et al., 2021). Since corporations are more likely to pay the ransom than individuals, they are the target of the new strain (Ibid). As the ransom message is written in German, it is thought that the Chimera ransomware predominantly targets German businesses (Ibid).

The 2016 ransomware known as Jigsaw was also known as BitcoinBlackmailer. It solely targets Windows-based machines for attack (Naseer et al., 2020). Via spam email, Jigsaw enters a system through Adware and downloads from porn sites both of contain ransomware variants (Alzahrani et al., 2020). The Jigsaw installer is included in the attachment or download and will launch once the file has been opened. The ransomware employs Advanced Encryption Standard (AES) encryption and encrypts all of the computer's data files as well as the Master Boot Record (Craciun, Mogage and Simion, 2018). Additionally, it makes sure the machine starts up with it. Once the application is installed, encryption begins instantly (Ibid).

2.4.3 Botnet Software

Botnet software or bots are significant threats to the security status of information systems and organisations as they act as a remote control or launcher of other illegal malicious attacks such as spam, click fraud, data, or identity theft, phishing, DDoS, and other malware attacks (Alieyan, et al., 2017). The report published by Wong (2016) explained that botnets are compromised devices which can be a WIFI router or a laptop found next door. The study further noted that these devices come with basic security and are vulnerable to exploitation. With a collection of bots, the botnet can be composed, and a

large-scale distributed DDoS can be started that can impact websites, and hinder business operations by making them offline (Wong, 2016).

Li et al., (2019) argued that IoT-based botnet is among the emerging threats to cybersecurity as an increased number of insecure devices are connected to the public network and they are vulnerable to botnet software. Concerning the dynamic digitally driven business environment of UAE, the GCC countries, in general, are a potential target for cyberattacks, especially in terms of botnets. According to a survey by Norton by Symantec, Riyadh is the GCC's top city for bot infections, and the capital of Saudi Arabia is also the fourth-most bot-infested city in the Middle East with 43.1% of the region's bots. According to a survey done by Norton by Symantec, a top cybersecurity company, Dubai, United Arab Emirates, was the second most bot-infected city in the GCC and the sixth most bot-infected city in the Middle East, with 24.7% of bots in the area (Trade Arabia, 2017).

Furthermore, the article claimed that DDoS attacks executed using botnets create huge disturbances, some of the attacks were on the botnet Meris which is strong enough to send massive requests in one-second Trade Arabia, (2017). The study by Yamaguchi (2022) discussed other botnets like Meris. As per Wang, an active botnet known as Meris, which is also Latvian meaning plague, is responsible for a recent wave of DDoS attacks that have been directed against thousands of websites all around the world (Yamaguchi, 2022). It was first discovered by QRator in late June 2021 during a cooperative study they carried out with Yandex (Ibid). The study also discussed popular botnet attacks such as Methbot in 2016, Mirai in 2016, and 3ve in 2018 (Yamaguchi, 2022).

Agreeably, White Ops (2018) discussed that Mirai in 2016 was the activator of a massive DDoS attack on the U.S. leaving a large portion of the internet inaccessible; the worms used to infect Internet of Things **(**IoT) devices infected more than 600,000 devices and bringing massive disturbances. (Kolias et al., 2017). The software known as Mirai attacks consumer electronics like cameras and wireless modems and transforms them into zombie networks of remote-controlled bots (Ibid). Cyberattackers strike pcs and other electronic devices with large-scale DDoS assaults using Mirai botnets (Kolias et al., 2017). Similarly, Methbot was the greatest botnet used to deceive the advertising business, allowing intelligent bots to view 300 million video ads daily on fake websites that were designed to seem like genuine publishers. The spoofing involved around 6,000 premium domains (Lu and Wang, 2016). 3ve Botnet was the most sophisticated and recent one which has infected over 1.7 million PCs worldwide which cost millions to advertisers and remains a major challenge for the advertising industry (Wang et al., 2018). 3ve functions in a unique manner. It made use of Google AdSense participants' phoney and subpar websites (Ibid). Then it offered false premium traffic for sale to advertising and successfully mimic the domains of eminent and well-regarded publications, fooling advertisers into believing they

were getting a deal (Ibid). Tens of thousands of infected PCs allowed 3ve to generate many fraudulent ad clicks, which was how the operation generated revenue (Wang et al., 2018).

2.5 Vulnerability Due to the Internet of Things (IoT)

With the rapid advancement and increased reliance on the internet and computing devices, security threats have become serious and produced a significant threat to the future of the Internet of Things (IoT) (Miloslavskaya and Tolstoy, 2019). According to Wong (2016), IoT encompasses the reliance of devices on the internet with 24-hour connectivity and thus the cyberattack on these devices is also likely to break all the previous serious cyber threats or cyber events. An example to demonstrate the severity of the issue is autonomous vehicles where sensors can be attacked by a hacker and turned against the driver leading to injuries or death (Mishra and Pandya, 2021). The situation of cybersecurity has worsened and the attacks have become severe and sophisticated due to the emergence of novel technologies like blockchain and IoT (Huxley, 2022). Figure 2-4 shows the countries facing the highest number of IoT-based cyberattacks from the medium of the internet in 2016 (Barnard, 2016). UAE has the second-highest percentage of IoT-based cyberattacks among other countries such as (22.8%). Qatar has witnessed the highest number of cyberattacks at 24% with Egypt having faced 17.9% of IoT-based cyberattacks in 2016 (Barnard, 2016). A lot of novel devices are being used by users in UAE for various applications like controlling the lighting, fridge, cooling, etc. (Barnard, 2016).

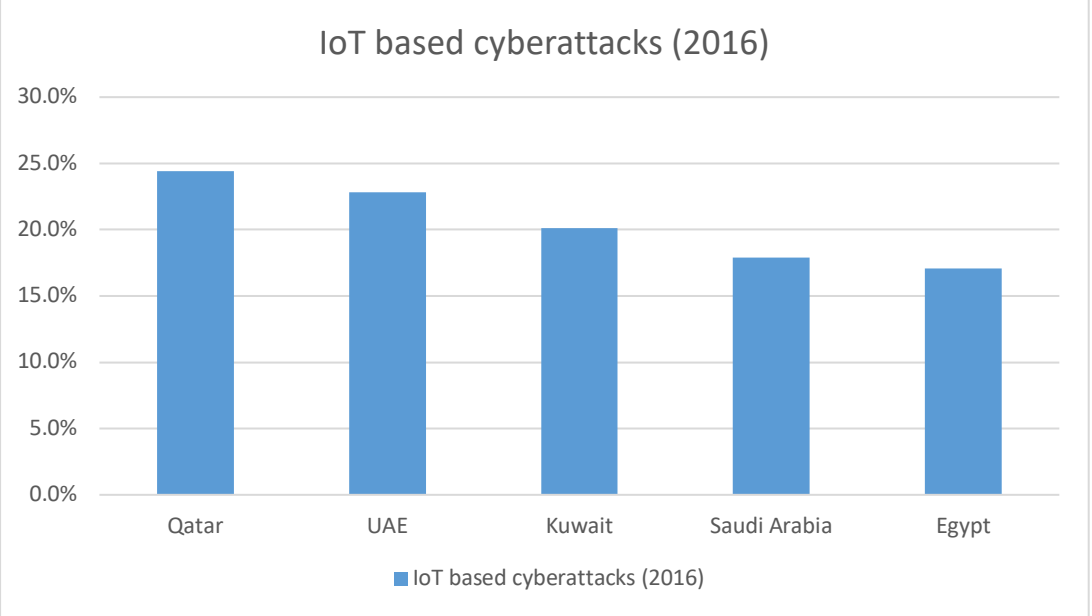

Figure 2-4: Cyberattacks in 2016 in the Middle East Source: (Barnard, 2016)

The report published by Digital14 (2020) surveyed the cyberattacks commenced on IoT devices such as security locking systems, voice controller control panels, surveillance cameras, and Heating,

Ventilation, and Air Conditioning (HVAC) systems on daily basis and found that UAE is particularly at risk because of the greatest number of insecure devices vulnerable to botnet-based IoT cyberattacks.

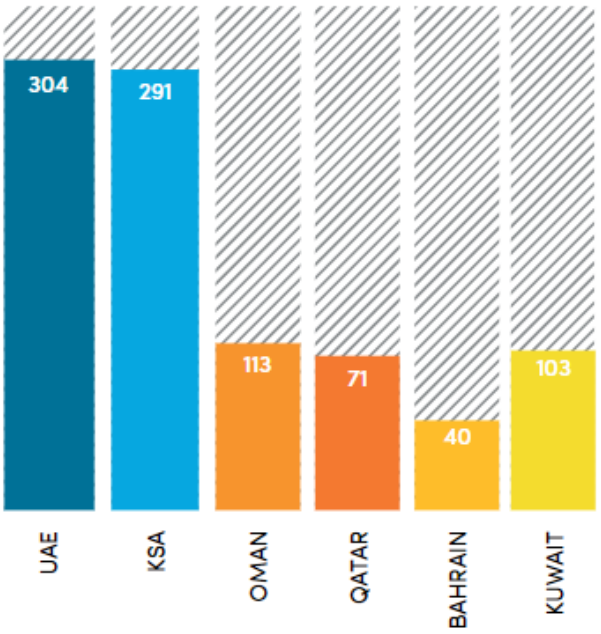

Figure 2-5: Daily Internet of Things Attacks (Average) by Country Source: (Digital14, 2020)

Figure 2-5 shows the number of attacks conducted on different countries such as KSA, Oman, Bahrain, Qatar, Kuwait, and UAE on daily basis. It is assessed that UAE is the greatest target, in addition to KSA, on average 304 and 291 attacks on IoT devices are commenced on daily basis, respectively. The cyberattacks on IoTs in the UAE are the greatest among all the GCC countries and this presents the case for existing compromised IoT devices to expand and attack other connected devices threatening the cyberspace ecosystem.

Although there is a general acceptance of the vulnerability of SMEs to cyber threats in much of the literature, there is a differing view on the causes and the effective countermeasures. As an example, Aldawood and Skinner (2018) note human factors and staff ignorance as their key weaknesses, but Jamil et al. (2024) and Norman et al. (2015) attribute the failure of SMEs to be cyber prepared to structural constraints, including budget, expertise, and risk perception. Rose et al. (2020) and Ahdadou et al. (2022), on the contrary, develop the resilience-based viewpoint, which implies that SMEs may offset resource scarcity with the help of adaptive capacity and policy reinforcement. This break shows a theoretical conflict between behavioural accounts and frameworks of capabilities. The current research synthesises all these views by using Protection Motivation Theory (PMT) to study behavioural intentions and relating it to Digital Resilience Theory to reflect organisational learning and flexibility in the long-

run. This synthesis transcends a list of challenges to an assessment of the ways psychological, and systemic factors interact to contribute to SME cyber-preparedness.

2.6 Vulnerability Due to Human Error

The information security vulnerabilities have increased due to human error such as sending critical emails to the wrong person, exposing passwords and other credentials to external parties unintentionally, failure to use, inappropriate actions while handling the information system and a lack of awareness regarding the importance of cybersecurity (Kraemer and Carayon, 2007). A survey by Kaspersky Lab noted that employees' lack of awareness was among the most prevalent challenges and issues of information security (Sadaqat, 2021). Similarly, the report published by Association of Chartered Certified Accountants (ACCA) Global (2016) also discussed the human-related vulnerabilities that maintenance regimes are not religiously followed by staff and employees in SMEs.

Discussing the factors behind human-related cybersecurity vulnerabilities, Fawcett (2020) argued that part of the overall problem and challenges to information security is due to human errors and a lack of awareness regarding information security practices. For instance, the staff in SMEs disregard the importance of cybersecurity, consequently, most computing devices are insecure due to outdated operating systems or old software and security patches (Ibid). As mentioned by Shepherd (2022), cybercriminals make use of the loopholes found in the old security patches of various software to execute cyberattacks on SMEs and large organisations. About 50% of the total attacks conducted on businesses in the Middle East region were because of outdated patches or unpatched weaknesses (Zawya.com, 2022). This indicates that human-related vulnerabilities have worsened the issues and challenges of cybersecurity in the SMEs of Abu Dhabi (Ahmed and Nanath, 2021). In this regard, Macaulay (2017) stated that unpatched systems are among the major challenges and greatest weaknesses that are exploited by attackers. Furthermore, it is mentioned in the study that patch management, software updates, and security patching are timely conducted by appointed individuals to comply with security policies and organisational requirements.

The study by Jartelius (2020) argued that employees make mistakes that impact the cybersecurity of the information systems leading to data breaches that are exploited by cyberattackers. Alsharif, et al. (2021) discussed human-related errors (unintentionally exposing critical information to a person outside the organisation or sending a critical email to the wrong person) and the factors leading to vulnerabilities, a survey was conducted by 333 participants regarding the awareness level regarding different cyber threats and security measures. It was found that overall awareness of cybersecurity practices is lacking among male and female employees (61%), Figure 2-6 is high and alarming. Furthermore, awareness regarding social engineering (37%), social platforms (35%), weak passwords (30%), and phishing attacks (30%) were also found to be higher followed by email usage (22%), data protection (29%) and

anti-virus (33%) measures. The study claimed that employee training and traditional security practices are inadequate and ineffective in ensuring cybersecurity (Alsharif, et al., 2021).

Similarly, the study by Rashkovski et al. (2016) provided different examples of human errors and practices by employees that makes the business information vulnerable to threats, for instance, sending personal and confidential information to the wrong email address. The example demonstrates employees' carelessness during business activities, sometimes they tend to use the suggested email without checking if they are indeed sending the information or confidential file to the targeted address. Correspondingly, Yıldırım and Mackie (2019) stated that employees use easy and predictable passwords which become easier for attackers to gain access to their accounts and misuse business-sensitive information.

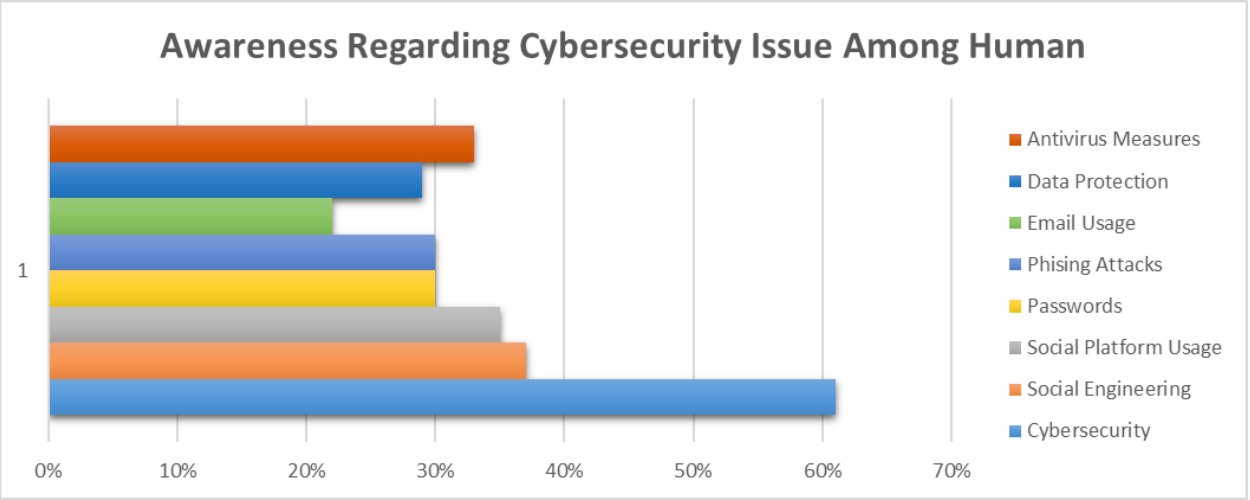

Figure 2-6: Awareness of Cybersecurity Issues among Human Source: (Alsharif, et al., 2021)

2.7 History of Cyberattacks

The world has witnessed cyberattacks like the Sony hack, Equifax breach, WannaCry, and others that attacked countries such as the USA, UK, UAE, Ukraine, India, Japan, Russia, Canada, etc. (CSIS, 2022). Equifax revealed a data breach in September 2017 that resulted in the exposure of 147 million people's personal data (Gressin, 2017). As per Gressin, the firm and the Federal Trade Commission have reached a global settlement, up to $425 million of the settlement would be used to assist those who were impacted by the data leak (Gressin, 2017). Towards the end of November 2014, a group identifying itself as the Guardians of Peace breached Sony Pictures Entertainment. Huge amounts of data were stolen from Sony's network by the hackers, who are widely thought to be affiliated with North Korea in some way. They disclosed the information to journalists, who then published the embarrassing remarks Sony staff members had made to one another (Sullivan, 2015). In May 2017, a global epidemic known as WannaCry ransomware struck. Through Windows-powered PCs, this ransomware threat propagated.

The hostage-taking of user files and the subsequent demand for a Bitcoin ransom (Chen and Bridges, 2017). By doing cyber threat's history writing, the attention can be drawn to how right now, in the digital era, new specific weaknesses are being created, especially in the context of this COVID-19 time digitalisation. Attributable to such histories, there would be the fundamental bases for the development of suitable cybersecurity strategies and policies that are tailored to the specific challenges that SMEs with regard to technology face in today's times.

Cybersecurity and information management practises among SMEs have been explained using a number of theoretical frameworks. Technological adoption has been studied through the Technology-Organisation-Environment (TOE) model (Tornatzky and Fleischer, 1990), which evaluates the organisational preparedness and environmental demands (Ahdadou et al., 2022). The Socio-Technical Systems Theory emphasises the interrelationship among people, processes, and technology as important in the development of information security culture (Leavitt, 1965) whereas the Resource-Based View (RBV) points at internal capabilities and knowledge as a primary factor in the maintenance of competitive advantage (Barney, 1991). Nevertheless, the frameworks deal more with structural or resource determinants and provide less information on individual behavioural motivations, which is a key factor in SMEs where decision-making is often owner-led (Jamil et al., 2024). That is why the Protection Motivation Theory (PMT) (Rogers, 1983) has been chosen as the primary theoretical framework, as it reflects how the cognitive beliefs about threat, efficacy, and vulnerability of the SME leaders contribute to the security-related intention and behaviour. The research uses Digital Resilience Theory (Rose et al., 2020) to complement PMT to include organisational learning and adaptive capability standpoint, thereby reconciling behavioural and systemic perspectives of SME cybersecurity preparedness.

2.8 Digital Adoption during COVID-19 in the UAE

During COVID-19, countries across the globe implemented security measures such as social distance policies (which include travel restrictions, quarantines, the closing of workplaces and schools, staying at home, maintaining 6 feet distance and so on) and lockdowns, SMEs consequently moved their business operations online (Cusmano and Raes, 2020). According to the World Digital Report, the UAE had the most rapid and highest digital adoption across the region (The National, 2021). The report also showed that 97.6% of individuals in the UAE own a smartphone or mobile, the average UAE residents were determined to spend about 320 million hours on smartphones and other devices facilitating internet usage (The National, 2021).

As mentioned by Nuseir (2018), SMEs transformed their services to go online to increase their finances and bring operational efficiency to their transactions. The current business market has increased reliance on analytical data and information systems (Ahmed and Nanath, 2021). Thus, the increased

digital adoption in SMEs exposed them to attacks and vulnerabilities producing the biggest threat to information and Cybersecurity. Kamel (2021) argued that due to the increased digital adoption during COVID-19, UAE businesses have become susceptible to cyberattacks because more employees work remotely from publicly exposed networks.

2.9 Cybersecurity Issues in the UAE

2.9.1 Cyber threats in the UAE

In UAE, the rate of cyber threats has been on the rise as technological advancements were implemented rapidly in various sectors of the country such as oil and gas, manufacturing, and hospitality sector (Ahmed and Nanath, 2021). Guven (2018) argued that official data from governmental sources in UAE related to cybercrimes are not officially found but news articles and media contributions enlighten the subject (Ibid). UAE has become a significant target for attackers with an increase of 4.3% likelihood for the country's vulnerabilities as social media penetration and technological reliance is expanding (Hakmeh, 2017). Concerning this, Guven (2018) also found that the causes behind this likelihood include technological adoption, increase smartphone and internet penetration, and reputation across the globe. In 2019, UAE experienced more than one million incidents related to phishing and more than 23 million incidents of malware attacks (Huxley, 2020).

The Kaspersky Lab report (2015) ranked UAE in the 19th position on the list of countries that are greatly exposed to cyber threats due to infrastructural susceptibilities. Furthermore, the examination of the local threats level for the UAE revealed that the country suffered more than 52% online injections in 2015 producing a higher risk (Kaspersky Lab report, 2015). In 2021, Iranian hackers attacked agencies of the UAE government and companies (associated with oil and gas production) in academia in the UAE and other countries during a campaign of cyber-attacks (CSIS, 2022). Due to the attack, UAE critical firms have lost some critical information regarding the oil and gas sector. However, the attacks were identified in the earliest stage which restricts the attacker's objectives (Ibid).

Social media penetration is also found to be higher in UAE, compared to other countries, such as 98.98% of the total population (Fawcett, 2020). This indicates that almost everyone in the country has a social media presence producing the greatest risk for these individuals to be victims of social engineering attacks (Ibid). The article published by Al-Monitor (2020) demonstrated that cyberattacks in UAE increased by 250% during the COVID-19 pandemic. This claim aligns with the figures in a report published by Clarke (2021) declaring that Dubai Police registered more than 25,000 cybercrime reports during the pandemic in the UAE. Moreover, the cybercrime reports increased annually since the inception of the Cybercrime Department, Figure 2-7 below shows the findings of the study using a graphical representation (Clarke, 2021). Cybercrimes in UAE were highest for the year 2020 such as

25,000 reports, followed by 2019 with 14,000 cybercrime reports, and in 2018 less than 5,000 cybercrimes were reported to the respected department.

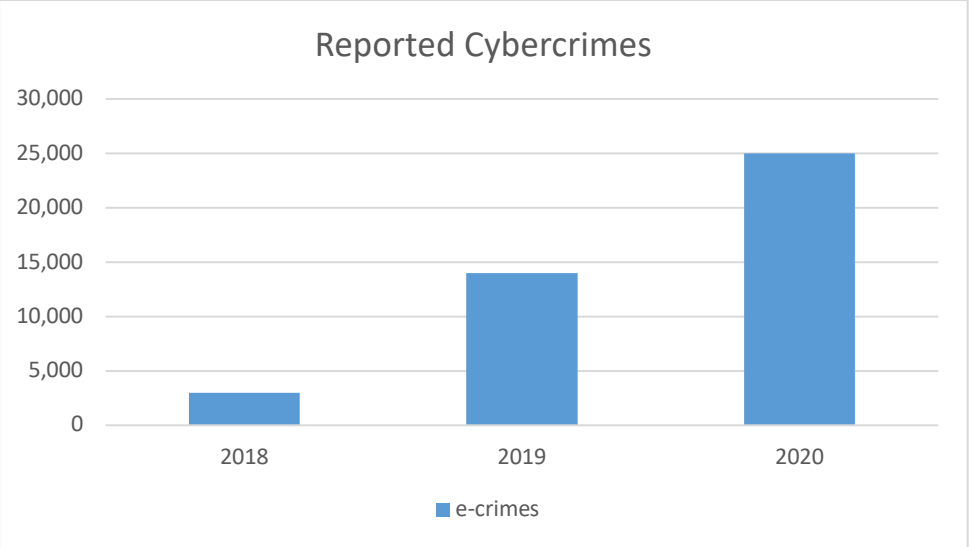

Figure 2-7: Reported Cyber crimes Source: (Clarke, 2021)

2.9.2 Information Security Challenges in SMEs of UAE

SMEs are most vulnerable concerning information security mainly because of inadequate cybersecurity measures and ineffective policy frameworks (OECD, 2021). In addition to this, the study by Yuwen et al. (2016) stated that SMEs are more prone to cyberattacks because they have poor business continuity planning, weak and inadequate crisis management and risk management strategies. It is assessed that the SMEs have weak financial infrastructure, and low funds to spend on information security measures; the staff is fewer and thus they are most likely to believe that they are safe (Wamda, 2022).

Supporting this, Marks and Thomalla (2017) found that SMEs lack the resources and human expertise required for effective cybersecurity and are susceptible to disruption, and internal and external inconsistencies. Agreeably, a report by the Federation of Small Businesses (FSB) on cyber-resilience showed that 66% of SMEs became victims of cybercrime in the years between 2014 to 2015 due to a shortage of necessary resources (ACCA Global, 2016). The report also determined from a survey by Cyber Security Breaches that 69% of SMEs considered information security a high priority, only 29% implemented formal plans and policies of cybersecurity, whereas 10% had the incident-management action plan in place (ACCA Global, 2016). Furthermore, Ahmed and Nanath (2021) highlighted that most SMEs do not have a separate in-house department to deal with cybersecurity vulnerabilities due to a lack of funds. Most SMEs cannot survive after the first attack leading to substantial data loss and the average time of survival is assessed as two months as mentioned by a report published by (Better

Business Bureau, 2017). It is assessed that SMEs ' cybersecurity measures are not efficient and effective in securing their business-critical information (Zarrouk et al., 2020).

Extant studies including Marks and Thomalla (2017) and OECD (2019), noted that information security challenges faced by SMEs in the UAE can be categorised as shortage of resources, lack of awareness, reluctance towards adoption of new technologies and a skill-set shortage to address information security issues and bring creative solutions. Wamda (2022) claimed that access to finance is the major barrier that stuns the growth and development of SMEs in the UAE towards secure and safe information security practices and measures. It is further stated that SMEs face a challenge in acquiring funds due to their lack of history, formal documentation, and information symmetry. The claims in the article are also explored by a survey conducted by MasterCard (2021), the findings indicated that 60% of the SMEs operating in UAE stated that the biggest challenge is to maintain and expand their business. About 61% determined that business costs are rising whereas 38% mentioned that they needed easier and barrier-free access to funds and capital.

Aligning with these findings, Zarrouk et al., (2020) focused on the case of UAE SMEs to analyse how financial resources impacted their performance. The interviews conducted with 27 participants suggested that the financial resources have a significant impact on the SMEs' performance and played a mediating role in impacting entrepreneurial orientation indicating the survival of business becomes challenging. While these studies demonstrate the financial aspects as being more challenging, the report by The Economist Intelligence Unit (2017) presented a different argument. It is mentioned that UAE is facing a challenge regarding the computer science skills in its workforce such as 2% population is digitally talented. This national issue has brought human-expertise-related barriers for the SMEs in the UAE contributing to information security challenges (The Economist Intelligence Unit ,2017).

The information security challenges in SMEs currently are regarding the lack of awareness of the importance of cybersecurity and the lack of funds or investments to ensure the best information security standards (Zarrouk et al., 2020). SMEs do not take the information security challenges and threats seriously as previously mentioned (MasterCard, 2021). Furthermore, there is a false belief that cyberattacks are more inclined to attack a large organisation compared to SMEs (Sharma, 2021). Ahmed and Nanath (2021) mentioned one of the reasons behind attacking SMEs is because of the business relationships they maintain with large companies; thus, SMEs are used as a gateway to execute a large attack. Therefore, there is a need to increase the awareness among the employees and staff of SMEs in the UAE as it has contributed to the challenges faced by them to combat cyber threats and vulnerabilities (Ahmed and Nanath, 2021).

2.10 UAE Cybersecurity Policies

Countries, worldwide, have started focusing on the problem of cybersecurity as it has become aware of the grave consequences (Sullivan, 2015). For instance, hackers can use the data of citizens or employees to achieve desirable results in their malicious Artificial intelligence (AI) programmes (Sharma, 2021). As COVID-19 forced several companies in the UAE and worldwide to adopt digital communication technologies, the cybercrimes and cyberattacks rapidly increased in the country (Younies and Na, 2020). Due to the increased cybercrimes and cyberattacks in UAE, the government developed several strategies and measures to strengthen its infrastructure and information security defence system across all sectors (Sullivan, 2015).

Five key domains are implemented as part of the UAE Security Strategy (UAE Government, 2022). The first area is called the Cyber-smart nation, and its major goal is to increase public understanding of the value of cybersecurity and create a culture that is fully aware of the risks posed by cybercrime. It seeks to help individuals and institutions in the UAE acquire the knowledge and skills necessary to manage cybersecurity risks (UAE Government, 2022). The second domain is innovation, which focuses on scientific research and technological invention in the area of electronic security as well as the creation of a free, open, and safe cyber environment (UAE Government, 2022).

The third domain, known as cyber resilience, is where the continuity and reliability of IT systems are guaranteed in the case of any cyberattacks, with a primary focus on maintaining the adaptability of cyberspace (UAE Government, 2022). The goal of the fourth domain, which is cybersecurity, is to create a safe online environment by putting in place safeguards that ensure data protection, confidentiality, and availability (UAE Government, 2022). The fifth area is national and international cooperation in cybersecurity, which was developed to forge local and worldwide alliances and to strengthen frameworks of collaboration with various sectors at the local and international levels to address threats and hazards in cyberspace (UAE Government, 2022).

Initially, UAE started realizing the importance of cybersecurity in 2006 when it enforced laws against cybercrimes with the implementation of the first Federal Cybercrime Law (Rajan, et al., 2017). cybersecurity laws of 2006 has restricted various activities such as unlawfully gaining access to the system and website. In addition to this, data security laws are covered in 2006 cybersecurity laws (Federal Law 2006, n2). For example, destruction, deletion, erasure, damaging, disclosure, republication and alteration of data will be considered as a crime punishment shall be imprisonment for a term of at least 6 months and a fine or either (Federal Law 2006, n2).

These federal laws were later amended as per requirements in 2012 to the Federal Cybercrimes Law (5) (Al Antali, 2018). In 2016, the law was further amended to make the cybercrime offence a punishable act as per Article (1) – Federal Law (12) (Rajan, et al., 2017). A study by Al Antali (2018) compared

UAE's legal strategies against cybercrimes and concluded that the country is inexperienced and adopted the first law against cybercrime sixteen years later than the UK. On the other hand, the study by Younies and Al-Tawil (2020) explored current UAE cybercrime laws and examined how it protects its businesses and citizens from cybercrimes and threats. The cybercrime laws ensures that the offenders will be penalised with the strict penalties and fines as much as possible (Alketbi, Nasir and Talib, 2018). In addition to this, the implementation and rule of law also discourage online fraud behaviour (Rajan, et al., 2017).

It was found that UAE has implemented effective strategies and has taken preventive measures to prevent cybercrimes (Younies and Al-Tawil, 2020). Recently, the UAE government announced the budget of 290 billion dirham or 79 billion USD for cybersecurity for the coming years (2022-2026) which is the highest for all the gulf countries implying that country is serious about adopting security standards (Al-Monitor, 2020). Several measures have been taken by the UAE government to ensure cybersecurity and the protection of information across various sectors (Alketbi, Nasir and Talib, 2018). UAE's National cybersecurity Strategy (NCS) is developed in 2019 to create and maintain a safe and secure cyber environment using the pillars of strategy such as strengthening cybersecurity laws and regulations, an ecosystem of cybersecurity, a Critical Information Infrastructure Protection (CIIP) programme, partnerships, and a national plan for cybercrime incident response. (Younies and Al-Tawil, 2020). UAE Information Assurance Regulation (IAR) was developed to ensure a standardized level of information security and supporting system, aiming to promote a trusted cyber and digital environment across the country (UAE, 2022).

Although the UAE has developed and evolved its cybercrime laws and has set in place a national cybersecurity strategy, its legal framework is condemned by many scholars like Fawcett, and Al Antali. Fawcett (2020) pointed out some issues and inconsistencies in the regulatory and legal framework in the UAE related to cybersecurity. Referring to the cybersecurity ACT 2018 framework that allows regulation and licensing of cybersecurity services and the related professionals, the author mentioned that such a regulatory action if expanded can be risky for the UAE cyberspace ecosystem. Moreover, Fawcett (2020) identified another issue of the legal status of white hackers or ethical hacking that is employed in firms to assess the vulnerabilities of a system. As per the current framework and regulation, the laws regarding white hackers are not clear and direct (Fawcett, 2020).

Similarly, Al Antali (2018) argued that the UAE has no federal regulations regarding data protection while Article 31 advocating privacy rights of the citizens is also limited and not extendedly applicable for non-Emiratis residing in the UAE. This indicates that the regulatory and legal framework of the UAE regarding cybersecurity and information security requires careful consideration (Al Antali, 2018). Despite the challenges faced by SMEs in ensuring the information security standards, the policies and

regulations also play an integral role as ambiguity regarding policies can delay the process of security and enhancement in SMEs (Younies and Al-Tawil, 2020).

2.11 Information Security Practices in SMEs

According to Mrad (2021), due to the increase in cyberattacks during COVID-19 especially ransomware attacks, SMEs have become more sensitive to the importance of cybersecurity. Several documents and studies regarding cyberattacks on SMEs and their consequences have contributed to the overall awareness of SMEs towards cybersecurity (Shojaifar and Jarvinen, 2021; OECD, 2019; Verizon, 2019). To demonstrate the severity of cyberattacks conducted during COVID-19 on SMEs, the International Chamber of Commerce (ICC) launched a significant campaign with the notion "Save our SMEs" (ICC, 2020). The pandemic has made the SMEs and large corporations' managers aware of the security gaps, and correct information security practices that lead to increased cyberattacks (Alsharari, Al-Shboul and Alteneiji, 2020).

In response, the SMEs have come up with different information security practices such as a cloud-first approach, adoption of cloud technologies, and using a combination of technologies and tools (Firewalls, intrusion detection system, data encryption tools, antiviruses) to combat cyber threats (Ahmed and Nanath, 2021). Some of the SMEs in the UAE have shifted to more advanced technologies, like adopting cloud-based services, as many employees were required to work from a remote location exposing their business details to attackers via networks (Alsharari, Al-Shboul and Alteneiji, 2020). The authors Reyes et al. (2012) declared that cloud services can aid the problem of information security in SMEs as cloud security can enhance the overall security strategy of the SMEs saving them time and cost.

The current information security practices in the SMEs of UAE are ineffective and inadequate (Check Point Research, 2022). A report brought insights into the current information security practices in SMEs of the Middle East. The top-most information security solutions preferred by most organisations were firewalls and endpoint security measures (Shojaifar and Fricker, 2020). These findings indicate that firewalls and endpoint security are the most prevalently used information security practice in SMEs (Barker et al., 2014). In addition to this, Mansfield (2017) revealed that 86% of the SMEs use antivirus software such as Avast, Kaspersky, Bit defender, and so on as a precautionary information security measure because they do not have any other efficient means of handling cyber threats. The information security practices in the SMEs have evolved as previously the security was not prioritised (Ahmed and Nanath, 2021).

However, there is observed a gap between the awareness of the SMEs regarding the importance of cybersecurity and the current information security practices (Elbeltagi et al., 2013). While various studies reveal that SMEs face a challenge in balancing the adoption of advanced technologies and investing in

cybersecurity measures (Mrad, 2021), other studies have suggested that most SMEs only employ basic information security practices (Shojaifar and Fricker, 2020; Kabanda, et al., 2018). Ahmed and Nanath (2021) indicated the necessity of information security regarding network and physical security, few studies have provided a lightweight solution or information security tools that SMEs can implement (ENISA, 2021; Ruiz and Spain, 2020). For instance, SMESEC is a lightweight framework to protect SMEs against cyber threats (FHNW, 2020). The main reason for inadequate information security practices is the lack of trained staff, and awareness among the employees, in addition to a lack of funds to invest and ensure higher standards of information security (Ahmed and Nanath, 2021).

2.12 Cybersecurity risks 2021-2022

According to the research conducted by Palandrani (2022), the rising cybercrimes and the impact of these cyberattacks are likely to continue in 2022. According to the report for Forbes (2022), cyberattacks' prevalence and costly damages observed in 2020-2021 are likely to increase in 2021-2022, the average cost of the data breach was examined to increase from 3.86 million to 4.24 million USD from 2020 to 2021, respectively (IBM, 2021). A report authored by Novinson (2021) and published by Computer Reseller News (CRN), an American computer publication, discussed the top 10 cyberattacks of 2021 claiming the food production, firms, and especially the technology sector was hard hit with approximately. 320 million USD of ransom money. Palandrani (2022) discussed the findings of the CRN report and provided details regarding the top cyberattacks of 2021 along with the company name, industry, date, and the ransom money demanded from the victims (Table 2-2).

Table 2-2: Top 10 cyberattacks of 2021, Source: (Palandrani, 2022)

Major cyberattacks of 2021	Industry	Date (M/D/Y)	Ransom Money in Millions ($) demanded or paid
Microsoft Exchange	Technology	1-5-21	Undisclosed
Kia Motors	Automative	2-13-21	$20.00*
Bombardier	Manufacturing (Aviation)	2-23-21	Undisclosed
CNA Financial	Financial Services	3-21-21	$40.00
Harris Federation	Education	3-29-21	$8.00*
Colonial Pipeline	Energy	5-7-21	$4.40
Brenntag	Chemicals	5-11-21	$4.40
Kaseya	IT	7-2-21	$70.00*
Accenture	Technology	8-12-21	$50.00*
Acer	Technology	10-5-21	$50.00*

*Indicates that the amount was demanded but paid partially.

It can be seen in the table that ransom money is in millions between 20 and 50 million USD indicating the severity of damage to the financial situation of the businesses. All the cyberattacks were conducted in 2021 on different industries such as Finance, Food, Technology, Aviation, etc. It should be noted that the top attacks mentioned above were conducted on large corporations like Microsoft, Acer, Accenture, Kia Motors, etc. On the contrary, SMEs were hard hit during 2019- 2020 as COVID-19 impacts became prominent, an article by Towergate (2020) claimed that 65% of SMEs experience cyberattacks on average higher than 46% of all size businesses. The article published by The Economic Times (2022) also stated that small businesses are the potential targets while pointing out risks related to cybersecurity in 2022 for SMEs. The article mentioned that remote-work attacks, cloud vulnerabilities, IoT vulnerabilities, Ransomware attacks, and credential stuffing for a data breach are among the topmost trending risks for 2022.

A survey conducted by World Economic Forum (WEF) (2022) based on 120 cyber leaders from 20 different countries also found that among the cybersecurity outlook for 2022, the trends related to SMEs suggest: i) ransomware attacks are considered dangerous by 80% of cyber leaders while 50% responded that ransomware attacks are expected to continue in 2022. ii) SMEs will act as a key threat to partner networks, entrepreneurial eco-system, and supply chains as 88% of survey respondents showed their concern over cyber resiliency in SMEs. iii) 81% of experts suggested that digital transformation is likely to improve cyber resiliency in SMEs and other organisations. The trends related to cybersecurity risks in 2021-2022 also highlighted the trends related to malicious agents aiming to continue damaging critical infrastructural SMEs across the globe (The Economic Times, 2022). Idir and Karim (2021) claimed that cyberattackers are usually nation-state agents, foreign powers, or political activist groups that aim to cause harm and damage to the critical infrastructural firms in the UAE. Also, Mandiant (2022) provided its outlook on major nation-state malicious agents and name the big four such as Russia, Iran, North Korea, and China to continue cyberattacks in 2022.

2.13 Digital Security risk/ models/ strategies

Hassan et al., (2020) highlighted that COVID-19 has exposed businesses and the general public to the internet and digital technologies increasing the risks of cyber threats, a specific vulnerability to cyberthreats was determined in children and teens/youth of UAE. Thus, a Child Digital Safety Programme was launched and introduced to parents and children to ensure a safer and more secure online experience for children (The National, 2019).

The establishment of a child digital safety project to assist shield kids from online dangers was announced by the UAE Government. The new programme was a crucial component of government initiatives to educate kids about the risks of the internet. As kids learn to use social media and the internet,

the programme hopes to instil "good behaviour and values." According to officials, its implementation will empower kids, promote social cohesiveness, and help develop a new generation of tech-savvy consumers (The National, 2019).

Indeed, the COVID-19 pandemic accelerated digital transformation worldwide and provided hackers with more opportunities to infiltrate systems across organisations of all sizes. The rapid expansion of online platforms and growing dependency on digital systems have exposed individuals and SMEs to significant cybersecurity risks, highlighting the urgent need for businesses to strengthen existing vulnerabilities. In response, the UAE government has introduced several initiatives, such as the Child Digital Safety Initiative and the Children's Digital Wellbeing Pact, to address cyber and online dangers affecting young internet users. These programmes aim to educate and sensitise children and teenagers about safe social media use and responsible online behaviour. Such efforts not only safeguard the immediate wellbeing of young users but also contribute to the creation of a more secure and resilient digital environment.

The SMEs business culture of Abu Dhabi is exemplified by the networking and trust aspect. This reinforces the unique business culture in Abu Dhabi and, more broadly, across the UAE as a whole. This cultural characteristic can be utilized not only to strengthen cybersecurity within the organisations but also in their subcontractors (Ahmed and Nanath, 2021). SMEs can come up with a comprehensive cybersecurity awareness scheme and its implementation by intertwining it into the world of business dealings and transactions (ADC, 2019). This cybersecurity defence mechanism can be made more dynamic by making it progressive. This embraces routine cybersecurity training for stuff and using of effective techniques of digital security as well as the leadership to ask stakeholders how they are dealing with cybersecurity (Abbas, 2021). Also, with the growing trend of evolving digital security models, SMEs, in this context, need to address this mighty challenge by applying a risk-based approach to cybersecurity (Boehm et al., 2019). Here, the identification of digital assets and systems weaknesses most sensitive and critical is highly critical, and later security measures prioritization is based on the various cyber threats' impact through which digital presence is affected. Hence, SMEs can invest in bettering the utilization of their resources and be able to make informed resolutions in their ability to address the most critical risks.

2.14 Abu Dhabi SMEs and Cybersecurity Culture

Neal (2016) pointed out that the business culture in Abu Dhabi is based on relationships instead of transactions. (Neal, 2016). Similarly, Sena and Bhaumik (2021) agreed that personal relationships are crucial to businesses in the UAE. It is assessed that spending time with business clients, shareholders, and stakeholders is considered to develop trust and harmony. Thus, a series of business meetings are

conducted, and several deals are made before the business or a venture is started (Neal, 2016). On the contrary, an analysis of the UAE business culture suggests that it is among the least corrupted country in North Africa and the Middle Eastern region (Transparency International, 2018). Aligning with this claim, the recent statistics by Trading Economics also showed that UAE is among the 24 least corrupt countries among the 180 countries (Trading Economics, 2022). Figure 2-8 displays the UAE's ranking on Transparency International, it is observed that UAE scored 27 in 2012 and achieved 24 scores in 2021. It should be noted that the scores are on a scale between 0-100 indicating less corrupted to highly corrupted (Transparency International, 2018).

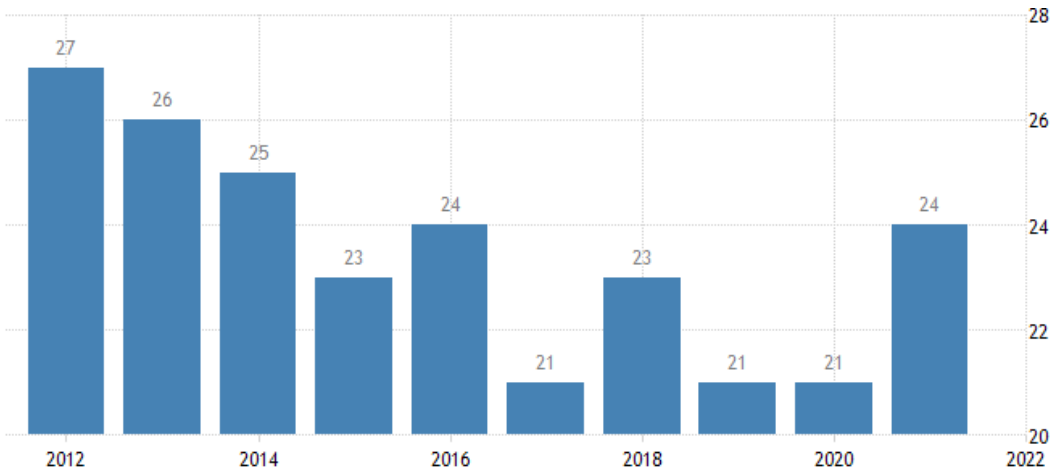

Figure 2-8: Corrupting Ranking by Country Source: (Trading Economics/Transparency International, 2022)

2.14.1 SME Market in Abu Dhabi

The study by Pinto (2016) argued that official data regarding the total number of SMEs in Abu Dhabi is lacking; however, non-governmental sources indicate that approximately 32% of the total SMEs in the UAE are located in Abu Dhabi, 45% in Dubai, and 16% in Sharjah. On the contrary, the report published by Gulf Capital (2019) claimed that 41% of the total SMEs in the UAE are located in Dubai, 23% in Abu Dhabi, and followed by 17% in Sharjah, with the remaining in Ras Al Khaimah and the other Emirates. The SME sector in Abu Dhabi is 98% of the economic structure if micro-companies are also included but there has been less economic activity related to SMEs as the economy is oil-dependent (ADC, 2019). Sharma (2022) elaborated that in 2018 the total number of SMEs in Abu Dhabi was 54,234. Figure 2-9 shows the breakdown of the total SMEs in Abu Dhabi based on size such as micro, small and medium enterprises. It can be observed that, in 2018, there were 33,760 micro, 18,945 small companies, and about 1,529 medium-sized organisations operating in the UAE. According to the report

published by The Abu Dhabi Chamber (ADC) in (2019), the Abu Dhabi government has prioritised the development of SMEs as it accounts for 29% of the total Gross Domestic Product (GDP).

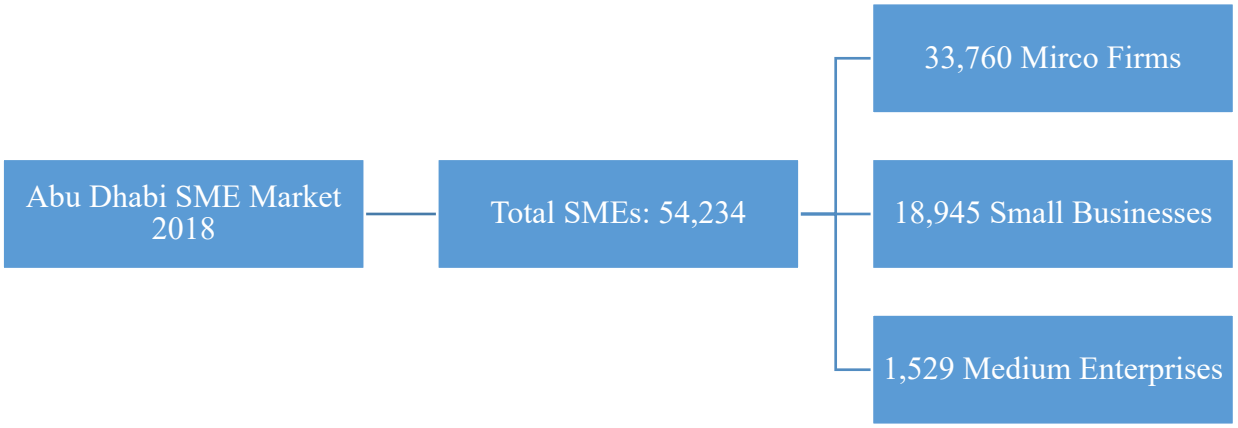

Figure 2-9: Abu Dhabi SME Market Source: (Sharma, 2022)

2.14.2 Cybersecurity workshop in Abu Dhabi

A workshop on cybersecurity, Association for Computing Machinery (ACM) Cyber-Physical Systems Security (CPSS) was held in Abu Dhabi in 2017 (ACM Digital Library, 2017). The proceedings attracted 35 submissions which were all related to the importance of cybersecurity, the increasing threat to cyber-physical systems (collections of physical and computer components with complete integration), reverse engineering (the process of taking a piece of hardware or software and examining its information flow and functionalities to comprehend its functionality), detecting cyberattacks using human behaviour, growing concern over IoT vulnerabilities, improving data validity, and attacks on data availability was discussed (ACM Digital Library, 2017).

Abu Dhabi has conducted various workshops and conferences between 2021 and 2022 to ensure awareness regarding cybersecurity and related challenges to stimulate the process of acquiring the best solutions (Atoum, Otoom and Ali, 2014). Conferences such as Abu Dhabi Investment and Business Council (AIBC) Asia Dubai, Gulf Information Security Expo and Conference (GISEC) Global 2022, Blockchain Summit Series Conference, and so on are important for cybersecurity awareness. As mentioned before, a large portion of the economic growth in Abu Dhabi is driven by the oil and energy sectors (ADC, 2019). Therefore, the Emirate engaged in workshops and conferences to identify and address the gap in the research and development related to cybersecurity challenges and solutions (Atoum, Otoom and Ali, 2014).

2.15 Effects of cyber-crimes in the UAE

Cybercrimes and financial breaches are among the greatest threats to the national security of the UAE and other countries in the MENA region (Younies and Al-Tawil, 2020). UAE has been affected by cybercrimes which should be mitigated by strengthening the laws and regulations in the country

(Debusmann, 2017). According to a publication by McKinsey and Co. (2020), a technology firm in UAE, 5% of all the global cyberattacks in 2017 were encountered by the country. The firm also claimed a 55% increase in cyberattacks over a five-year period. A study by Salama (2016) agreed and discussed that UAE is in the 8th position by the percentage of people attacked via trojans in 2016. Similarly, Younies and Al-Tawil (2020) argued that the risks of trojans are higher in the country due to high smartphone users and penetration.

Concerning the effects of cyber-crimes on the UAE, Salama (2016) mentioned that the frequency and intensity of cyberattacks have impacted the country's digital and rapid transformation. Sami (2017) discussed the impacts of cyber threats on the UAE and mentioned that it has influenced and resulted in a series of cybersecurity strategies and legislative measures against cybercrimes. Younies and Al-Tawil (2020) confirmed that UAE has kept a large portion of the annual spending to invest in measures to strengthen cybersecurity.

A proactive approach in terms of aeCERT, a computer emergency response team, regulated by regulatory authorities in UAE is all set to help vulnerable systems against cyberattacks (Hudson, 2016). The article written by Agarib (2018) also discussed how cybercrimes have impacted UAE 's laws and regulations indicating that it has expanded to apply extreme sentences like deportation of foreigners involved in cybercrimes, confiscating malicious devices, and shutting down illegal websites, etc. The author Debusmann (2017) also stated on the effects of cybercrimes on the UAE that the country has become more sensitive to issues like misuse of social platforms, online devices, and websites considering them a threat to national security, conflicts among a diverse population residing in UAE and overall social stability of the country.

2.15.1 Tools to deal with the information security challenges during COVID-19

The study by ENISA (European Union Agency for Cybersecurity, 2021) stated that various cybersecurity tools (encryption, antiviruses, firewalls) can be used by businesses to address the challenges of information security such as antiviruses software, firewalls, Intrusion Detection Systems (IDS), email, and web protecting tools, backup tools (e.g., locked service cabinets, cloud storage), and encryption tools (e.g., BitLocker, VeraCrypt, LastPass). Rea-Guaman et al. (2018) demonstrated the importance of managing cybersecurity tools and employing multiple tools to ensure cybersecurity needs in SMEs are met. Related to this, Gourisetti et al. (2017) argued that in addition to using the mainstream tools of cybersecurity such as firewalls, endpoints security, and anti-virus, SMEs must also incorporate additional tools (packet sniffers, firewalls, and penetrating testing) to evaluate and conducted self-assessment and monitoring of cybersecurity tools. For instance, tools should be used to ensure an alert

that the anti-virus software is updated because outdated anti-virus software is less likely to detect malware effectively (Tully and Mohanraj, 2017).

2.15.2 Impact of modified practices on SMEs to address information security issues

The modified working practices influenced by the digital age such as vast amounts of information processing, and storing, across different channels like business organisations have impacted the information security practices (Lanz and Sussman, 2020). Previously, a simple firewall or a basic package of anti-virus software would be considered adequate (Kabanda, et al., 2018). Contrastingly, the advancement in digital technologies has influenced the need for information security advanced practices and measures to combat cyber threats (Davis and Pipikaite, 2020). Regarding this, Babbs (2020) stated that IT security is related to the overall approach to addressing information security issues focused highly on protecting the integrity, confidentiality, traceability, and availability of information technologies and systems. The following part presents the theoretical framework that supports the aforementioned discussion. The theoretical framework of this dissertation is comprised of a limited number of established theories, which will be examined and addressed in the coming sections.

2.16 Theoretical view

2.16.1 PMT Theory

The focus of Protection Motivation Theory (PMT) is the analysis of individuals' behavioural reactions and coping strategies within the framework of challenging situations (Norman et al. (2015). The current research examines the perspective of small and medium-sized firms (SMEs) in Abu Dhabi on their heightened apprehension towards the increasing cybersecurity threats. The concern stems from the rapid incorporation of digital technologies, notably in the context of the COVID-19 pandemic.

The Protection Motivation Theory (PMT) assigns equal significance to the notions of response efficacy, which refers to the idea that the suggested course of action would yield desired results, and self-efficacy, which pertains to an individual's belief in their own capability to carry out the advised action. In a similar vein, small and medium-sized enterprises (SMEs) evaluate the efficacy of information security management practices in addressing the potential hazards linked to the implementation of digital technology (Arroyabe et al., 2024). The self-efficacy of an individual refers to their level of confidence in efficiently implementing and maintaining these measures, along with the theoretical foundation of the Protection Motivation Theory.

The main assertion of PMT theory is that the motivating cause of the threat-appraisal process is that the threat triggers contributing toward the behaviour analysis and shaping (Wu, 2020). Rogers postulated the Protection Motivation Theory (PMT) in 1975 to explain why people feel driven to respond defensively when they sense a health threat (Sun and Shen, 2020). Over four decades, the utilisation of

PMT has expanded as predicted by Rogers. In the current context, cyber threats are taken into consideration thus five fundamental components of PMT are:

I. The perceived severity of cyberthreat incidents.
II. The likelihood of vulnerabilities to an incident.
III. Response efficiency.
IV. Self-efficacy.
V. Costs of response actions.

This study aims to investigate the impact of perceived threat and efficacy on the adoption of specific information security practises or solutions in response to the digital transformation accelerated by the COVID-19 pandemic based on the theoretical standing of PMT which is among the theoretical frameworks (among others, such as regular activities theory and the general theory of crime) that have already made a significant contribution to the study of cybercrime (Floyd et al., 2000). The strength of this paradigm is that it allows researchers to obtain a better grasp of the cognitive processes that decide the intention to take protective actions in the face of a threat (Kothe et al., 2019). This is an essential emphasis since perceptions of online risks and accessible coping techniques are thought to be the most important predictors of online protective behaviour (Norman et al., 2015). Furthermore, researching people's protective motivations in connection to cybercrime is extremely important, because these sorts of cyber dangers, individual actions may truly make a difference and increase online safety (Sommestad, Karlzén and Hallberg, 2015).

The Protection Motivation Theory is closely relevant to SMEs in the challenge of digital security, specifically under the impetus of the COVID-19 pandemic (Jamil et al., 2024). Although it was first developed to explain health-related behaviours, PMT has been notably extended equally well to explain behavioural responses toward cyber threats. This theory provides a robust framework from which perceived threats and efficacies of protective measures can be analysed for influencing security behaviour in organisations. Understanding these psychological drivers is important, as SMEs usually do not have the full range of security measures taken by a larger enterprise. The PMT was applied to explain cognitive appraisals leading to adopted or rejected security measures and provided insight into how SMEs can manage their cybersecurity risks.

PMT has continuously evidenced the effectiveness in predicting protective behaviours against cyber threats (Sulaiman et al., 2022). Such findings are of particular importance for the SMEs in Abu Dhabi, where rapid digital adoption has strongly increased the attack surface of cyber threats. With PMT, this study has been able to draw from a mature body of knowledge that integrates one model considering both cognitive analyses of the severity of threat and vulnerability, and perceptions of both the effectiveness and self-efficacy associated with the implementation of security measures. This has

importance in addressing specificity to the challenges experienced by SMEs, whose resource constraints affect the perception and implementation of cybersecurity solutions.

PMT enables an in-depth analysis of the behavioural responses to cyber threats by encapsulating the main elements, which are threat appraisal and coping appraisal (Vrhovec and Mihelič, 2021). From this theoretical perspective, it is feasible to not only examine the adoption of technologies but also the motivational spirit behind such an act-for instance, levels of responsiveness to cybersecurity policies and good practice. By focusing on these aspects, PMT serves to highlight the psychological barriers and facilitators that influence effective Information Security Management (ISM) within SMEs. This is of great importance in understanding how such businesses can surmount their limitations in terms of cybersecurity expertise and financial resource capabilities.

The flexibility of the PMT to incorporate additional variables makes it especially adaptable to new emerging contexts, such as in the digital transformation triggered by the pandemic (Ofosu-Ampong, 2021). This is important in testing how additional factors related to the dynamics introduced by remote work, changes in IT infrastructures, and increased reliance on digital communications modify cybersecurity behaviours among SMEs. Integrating these contemporary changes with traditional PMT constructs, such as perceived severity and self-efficacy, can add depth and applicability to your research in ways that are timely and relevant to current challenges.

It is worth mentioning that most research findings on cyberattacks and data security that use the PMT framework acknowledge the value of the theory, but also recognise the importance of extending and adapting the original framework to the online environment by including one or more additional variables, such as exposure to security media coverage (Sommestad, Karlzén and Hallberg, 2015), expertise with the world wide web (Rogers and Prentice-Dunn, 1997), past knowledge with cybersecurity risks (Floyd et al., 2000), electronic safe operation skills (Norman et al., 2015), or understanding (Norman et al., 2015).

These studies show that broadening the PMT framework leads to a better understanding of people's motivations for protection (Floyd et al., 2000). All of these studies, however, have one thing in common: they all look at how these new factors impact individual intentions and behaviours (Kothe et al., 2019). In contrast to innovative aspects, some traditional approaches will also need to be considered here to mitigate the cyber threats for SMEs.

2.16.2 Traditional Approaches to Mitigate Cyber Threat

Even though most organisations have numerous levels of defence such as authentication methods, Intrusion Detection System (IDS), and firewalls or their vital systems, assaults do occur (Barnum, 2012). Authentication methods provide access to relevant people through their identification and passwords,

firewalls filter out incoming data into the system's network, and IDS is a network security technology that was first developed to find application or computer vulnerabilities that may be exploited (Foglietta et al., 2018). System infiltration (attack on an information system) is often the result of a confluence of events rather than a single vulnerability being exploited for a cyberattack to succeed (Krishnan and Bhada, 2020; Digioia et al., 2012; Chin et al., 2012).

In all other terms, the harm is caused by the "total" of the attackers' conditions and actions (Greitzer and Frincke, 2010). Reductionism and Holism are two opposing theoretical approaches to object and system analysis and design (Kaloudi and Li, 2020). The Reductionists say that any system can be broken down into its constituent pieces and analysed that way, but the Holists argue that because the whole is larger than the sum of its parts, a system cannot be understood just via its parts (Acosta et al., 2020).

The present study employs a reductionist approach to analyse the complex network of elements that affect the consequences and long-term effects of COVID-19-related digital adoption on information security management in small and medium-sized enterprises (SMEs) in Abu Dhabi. The process entails decomposing intricate phenomena into more manageable elements to facilitate in-depth examination. In contrast, the application of Holism involves the consideration of variables and findings of a study within the wider framework of interconnected systems and socio-economic factors that impact the overall information security landscape in the region. This approach acknowledges the significance of a comprehensive understanding that goes beyond isolated components (Keller and Keller, 2019).

According to Foglietta et al. (2018), the reductionist approach is used in most current sciences and analysis methodologies, and it works well for understanding the behaviour of a wristwatch, an automobile, or the cosmic universe. Reductionism places a significant emphasis on causation or the idea that an effect has a cause (Greitzer and Frincke, 2010). The reductionist approach has drawbacks when it comes to emergent systems including human behaviour, socioeconomic systems, biological systems, and socio-cyber systems (computer systems with human involvement). The human body, a group of people's reaction to a political stimulus, the financial market's reaction to a merger, or a traffic bottleneck, none of these things can be anticipated by examining their parts (Roy and Xue, 2021). The historical-based approach to cybersecurity through a reductionist lens, focusing on particular point solutions for specific issues and attempting to predict how a cyber-criminal may target known flaws (Chin et al., 2012). It is past time for us to start thinking about cybersecurity from a different perspective (Digioia et al., 2012).

Device break-ins are similar to microbial infections in that they can spread the infection to a large portion of the population if they are "connected" to each other, and once detected, the systems are typically 'isolated,' and people are placed in 'quarantine,' to prevent the infection from spreading further (Acosta et al., 2020; Foglietta et al., 2018; Roy and Xue, 2021). Viruses, worms, diseases, and other

biological analogies are used in the language of cyber systems (Foglietta et al., 2018). Although there are numerous connections in epidemiology, the design ideas used in Cyber systems are not always matched with natural selection principles (Chin et al., 2012). This epidemiology is a revolutionary method for analysing and diagnosing cyberthreats and associated hazards, and it may be used in cybersecurity. It offers a methodical framework for analysing likelihood, consequence, management, and preventative interventions to study harmful behaviours like illness (Chin et al., 2012). Cyber systems rely heavily on the uniformity of processes and technological components, as opposed to the diversity of genes in a species' organisms, which makes them more robust to epidemic attacks (Schauer et al., 2019). In addition to the aforementioned perspectives, another perspective, there has been a strong need for a new approach to specifically address the complex nature of cyber threats being faced by SMEs.

2.16.3 Complexity-based Approach to Cyber Threats

Another theoretical approach to mitigating cyber threats is known as the complexity-based approach (Park and Lee, 2021). Complexity science approaches might be a beneficial addition to more conventional and traditional approaches (Swanda, 2016). This methodology entails comprehending and effectively handling cyber risks by taking into account the intricacies of the digital landscape. The authors of the study acknowledge the complexity and interconnectivity of contemporary IT environments, as well as the potential for threats to arise from several origins and manifest in various manifestations (Resende, Martins and Antunes, 2019).

The COVID-19 epidemic has expedited the adoption of digital technologies in several industries, particularly small and medium-sized enterprises (SMEs). The prevalence of remote-work, digital communication, and online business transactions has resulted in an increased scope for potential digital attacks. Pappaterra and Flammini (2019) argue that the growing usage of digital technologies can have implications for the management of information security within small and medium-sized enterprises (SMEs). The increased scope of potential vulnerabilities, combined with potential deficiencies in knowledge and infrastructure pertaining to Cybersecurity, might present novel obstacles for businesses in effectively protecting their digital resources.

Computer systems' adaptability makes them unpredictable since they are capable of emergent behaviour that cannot be anticipated without running it (Hodge et al., 2019). Running it in isolation in a test environment is also not the same as the actual thing; the apparent emergent behaviour is caused by the collision of many events (Gherbi and Charpentier, 2011). Under the complexity-based approach, the key preference is given to diversity over uniformity (Hamamreh, Furqan and Arslan, 2018). In biological systems, resilience to perturbations is important emergent behaviour (Siddiqui, 2016). Consider a species in which all creatures share the same genetic composition, body layout, antibodies, and immune response; a viral infection would wipe out the whole population (Park and Lee, 2021). But it does not

happen since we're all built differently and have varying levels of virus tolerance (Bopche and Mehtre, 2015).

Similarly, several mission-critical Cyber systems, particularly in the Aerospace and Medical industries, use "different implementations" of the same task, with a centralised "vote" mechanism deciding the answer to the requester if the results from the various implementations do not match. I It is customary for businesses to have duplicate copies of mission-critical systems, but sometimes they are usually homogeneous implementations rather than diversified ones, rendering them vulnerable to the same flaws and vulnerabilities as the primary ones (Bopche and Mehtre, 2015; Armstrong and Mayo, 2009). If the redundant systems are implemented differently from the primary systems – for example, with a different operating system, application container, or version of data - the two variations will have varying levels of resilience to specific assaults. On the versions, even a modification in the memory stack access sequence might affect the response to a buffer overflow attack (Armstrong and Mayo, 2009).

The Multi-Variant Execution Environments (MVEE) has been established, which allows apps with minor differences in implementation to run in lockstep and have their responses to requests monitored (Swanda, 2016). Bopche and Mehtre (2015) noted that MVEE have shown benefits in intrusion detection when attempting to modify the behaviour of the code or even finding existing weaknesses when the variants reply to a request differently. Using the N-version programming idea, Armstrong and Mayo (2009) asserted that at the University of Michigan, an N-version antivirus was constructed with heterogeneous implementations which includes several functional parts that are required to implement the entire framework that looked at any new files for corresponding viral signatures. In the N-version programming approach, N groups or individuals of developers who do not share the development process generate N-versions of software modules. The rationale behind this strategy is that various people would make different mistakes, thereby covering all possible points of failure (Armstrong and Mayo, 2009). Consequently, the anti-virus system is more durable, less vulnerable to internal threats, and has 35 per cent greater detection coverage across the estate (Mishra et al., 2020).

Another complexity-based cyber threat mitigation model is known as Agent-Based Modelling (ABM). According to Shafie-Khah and Catalão (2014), ABM is a modelling method for analysing and forecasting the behaviour of complex systems with adaptability features. Individuals or groups participating in the Complex system can be represented by artificial 'agents' who follow a set of established rules. Raiyn (2014) further added to ABM by saying that the Agents' behaviour might change and adapt depending on the situation. Simulation, unlike Deductive reasoning, which has been widely used to describe the dynamics of substantial socio-economic, does not attempt to generalise the system or the behaviour of the agents.

According to Schweitzer and Garcia (2010), ABMs have been used to research crowd management, disease transmission, market behaviour, and, more recently, financial risk assessments. It's a bottom-up modelling approach whereby each agent's behaviour is coded independently and can vary from that of other agents. Raiyn (2014) stressed the implementation point, stating that agents' evolutionary and self-learning behaviour may be implemented using a variety of methodologies, with the Genetic Algorithm being one of the most common.

Cyber systems, according to Armstrong and Mayo (2009), are links between software modules, the internet, logical circuit wiring, microchips, and a group of users and administrators. These interactions and players may be replicated in a model to do a "what-if" analysis and forecast the impact of changing parameters and interactions among model actors (Hamamreh, Furqan and Arslan, 2018). Secondly, Acosta et al. (2020) stated that simulation models have been used for analysing the performance characteristics based on application characteristics and user behaviour for a long time now – some of the popular capacity and performance management tools use the technique. Similar techniques can be applied to analyse the response of cyber systems to threats, design a fault-tolerant architecture and analyse the extent of emergent robustness due to the diversity of implementation (Park and Lee, 2021).

The "self-learning" mechanism of agents is one of the primary areas of interest in ABM (Acosta et al., 2020). An attacker's behaviour would develop with experience in the actual world (Siddiqui, 2016). Genetic Algorithms are used to accomplish this feature of an agent's behaviour (Shafie-Khah and Catalão, 2014). A genetic algorithm is an optimization approach that is based on natural selection, the mechanism that causes biological evolution. Such an approach is now being used in the cybersecurity world where systems optimise their security through natural selection (Mishra et al., 2020). They've been used to create vehicle and aeronautics engineering, improve Formula One car performance, and model investor learning behaviour in simulated stock markets (Shafie-Khah and Catalão, 2014; Raiyn, 2014).

2.16.4 Information Security Risk Management

Whitman and Mattord (2021) and Brecht and Nowey (2013) found that incentives that are not directly aligned with the human needs of many parties in information security make cyber risk management difficult in research on the management of information security risk. When a firm's security risk rises over a certain level, financial considerations may induce it to reduce its security expenditure, according to Layton (2016). Risk correlation, which they called interdependence diminishes a firm's incentives to spend on cybersecurity, as a result of companies' inclination to free ride on the protection provided by others' efforts (Kwon et al., 2007; Layton, 2016).

According to Brecht and Nowey, 2013, associated risk, attackers' income, and whether attackers may swap their efforts across different targets impact a firm's security effort. When attackers may switch

their efforts between targets, Calder and Watkins (2010) showed that organisations with powerful defences betray their protection levels to attackers. The sharing of information is a strategy for reducing the impact of associated risk (Layton, 2016). When companies exchange security information, Peltier (2005) discovered that unless adequate incentives are in place, they cut investments in information security.

Information security investments and secure exchange of information, according to Jones and Ashenden, (2005) serve as strategic complements. Secure exchange of information complements information security goals where a secured data transfer mechanism helps in achieving goals that are established by investing in information security (Ashenden, 2005). When the risk interdependence is negative, Kwon et al. (2007) assume that a business's security effort and information obtained from another firm are substitutes, and when the risk interdependence is positive, they are complements. The studies in this group solely studied self-protection as a risk management tool, not insurance, and hence do not give a comprehensive picture of risk management.

2.16.5 Risk-Based Approach to Cybersecurity

2.16.5.1 Phase 1: Initiate Business Impact Analysis (BIA)

Business Impact Analysis (BIA) is the first phase where a company determine and records critical processes in business and their related dependencies (Woolward, 2017). In BIA, the organisation needs to assess the identified risk and rank them based on their criticality (Paraskevas, 2020). Kwon et al., (2007) stated that the evaluation and ranking of different risks are based on the impact factor and probability of occurrence. For example, if there is a risk in the cybersecurity domain which can impact the organisation adversely and high chance of occurrence, the risk must be ranked higher (Blakley, McDermott and Geer, 2001).

Similarly, risk in the cybersecurity domain which a low impact on the organisational critical processes and the probability of occurrence is also low, the organisation can rank them to lower ranks. Related dependencies include non-technical and technical factors such as personal data, assets, organisational data, applications and facilities (Hoffmann et al., 2020). According to Spears and Barki (2010), during the BIA phase, the management will have an idea of how critical functions and operations might affect the business continuity if they were eliminated or hindered. Jones and Ashenden (2005) have critically evaluated the BIA phase and determined its outcome. According to them, BIA is the basic step towards the creation of a disaster recovery plan and business continuity managerial processes. With the help of BIA, the management is in a position to determine the critical processes and functions of a business and its supporting elements (Paraskevas, 2020). In addition, BIA helps management to understand the business environment and what type of risks are more important to address first for the sake of protecting it (Hoffmann et al., 2020).

2.16.5.2 Phase 2: Conduct and Perform Risk Assessment

Calder and Watkins (2010) stated that in risk management, the second step that management is required to take is categorised as a qualitative and quantitative approach or process that will facilitate identifying threats, regulatory requirements and vulnerability (Woolward, 2017). With the help of risk assessment, the management can statistically calculate, possible outcomes if identified threats and risks are actualised and generate a risk output value (Blakley, McDermott and Geer, 2001). According to Brecht and Nowey (2013), management and senior leadership can have the opportunity to understand and prioritise various risks present in the business environment with the help of risk output value. Spears and Barki (2010) argued that the risk output value is considered to be the major advantage of the risk management approach and facilitates generating personalised metrics especially related to the organisation. In addition, as compared to using generalised risk or off-the-shelf risk to organise particular cybersecurity programmes which might not comprehensively protect the firms from specific challenges, risk output value generates value addition to the risk management model (Paraskevas, 2020). Shedden et al., (2011) highlighted the importance of knowing the business risk and stated that it gives management power of a favourable position to rank vulnerabilities in a risk register (a document to record risk and its response).

In addition, they further stated that awareness regarding business risk helps the management to consolidate different risks and subsequent results are recorded in one place to ease accessibility issues (Tipton and Krause, 2007; Layton, 2016; and Peltier, 2005). Anderson and Moore (2006) put showed the importance of a risk register and stated that it provides actionable initiation for focusing strategic-based resources to reduce the impact of risks that pose a great threat to the business and its business continuity management plan.

2.16.5.3 Phase 3: Determine and Implement Required Controls

The third phase which presents various kinds of literature (Spears and Barki, 2010; Tu and Yuan, 2014; Shedden et al., 2011) put a strong emphasis on the implementation process. In this regard, management allocates responsibility and accountability to an individual, group or department to mitigate identified high-risk threats. According to Tu and Yuan (2014), the control process is regarded as an activity-based statement which aims to provide instructions regarding the mitigation and minimisation of security risks. Von Solms and Van Niekerk (2013) argued that an information security or cybersecurity framework can be used in the control process which includes the Health Information Trust Alliance (HITRUST), the Cybersecurity Framework (CSF), the National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53)), the Payment Card Industry Data Security Standard (PCI DSS) , the Control Objectives for Information and Related Technologies (COBIT), and

the Centre for Internet Security (CIS). These frameworks are known as the pre-packaged information security control for risk recognised by the industry, however, Da Veiga and Eloff (2010) stated that such frameworks can be customised for the organisation. Tipton and Krause (2007) studied the risk assessment plans where they stated that customised/personalised risk plans (risk management plans which are specifically designed for the company) help the management to personalise the control-related choices to meet identified threats and vulnerabilities.

In addition, personalised risks better enable the organisation to customise control choices to meet identified vulnerabilities and threats. Because the whole decision-making process is documented, it also allows the company to implement compensatory controls (Boehm et al., 2019). The documentation confirms that the organisation is aware of the hazard that the control is designed to address, and that alternative compensating measures have been properly implemented based on a cost-risk analysis (Layton, 2016).

As per the research of Calder and Watkins (2010), determining, and implementing an appropriate control process helps in providing a structure as well as an opportunity for the management to create "Standard Operating Procedures" (SOPs) that solidify and communicate the vision of the organisation and its priorities related to Cybersecurity. Similarly, Von Solms and Van Niekerk (2013) argued that a personalised control approach can help the management to achieve better compliance as it helps in creating opportunities for dialogue with various stakeholders. Therefore, a risk-based approach provides management and organisational leadership with a convincing rationale to adopt and adapt personalised control procedures along with concerns for indecision (Hoffmann et al., 2020).

2.16.5.4 Phase 4: Test, Validate and Report the Controls and Issues

According to Ohki et al. (2009), phase 4 where management and related cybersecurity and information security teams test security control and validate whether it is relevant and comprehensive or not and prepared a report if there are some shortcomings in the control mechanism. Shedden et al. (2011) argued that the testing and validation process is critical to entire security controls and it is considered the mandatory phase. The organisation can perform various types of tests such as penetration tests, vulnerability management tests, additional risk tests, internal audits, business continuity exercises, and compliance control tests (Peltier, 2005). Da Veiga and Eloff (2010) argued that every phase of risk management is a value addition process. For example, the validation and testing phase provides confidence to the management that their developed controls are comprehensively working and providing the required security (Von Solms and Van Niekerk, 2013).

Moreover, with testing, risk impact scores along with residual risk can be documented properly and can be added to the risk register for future requirements (Tipton and Krause, 2007). Based on the

investment of effort, time and cost for creating a new control mechanism, organisational risk rating would decrease by a significant margin and will be indicating a better and healthier risk profile (Peltier, 2005; Spears and Barki, 2010). As per Whitman and Mattord (2021), the Validation and testing process and related efforts must be reported and documented. In addition, the help of effective mechanisms of reporting will help the management demonstrate the progress of the management to executive leadership and business owners along with compliance with different legislative and regulatory bodies (Tipton and Krause, 2007). In addition to this, with the help of effective planning, a proper and comprehensive report helps in establishing a foundation for remedial measures against the knowledge and security gap in information management (Peltier, 2005).

2.16.5.5 Phase 5: Monitoring and Governance Procedures

Phase 5 which is categorised as the last phase in risk management for information and cybersecurity facilitate immortalising the first four-phase into a business process that can be repeated at a regular interval (Peltier, 2005). Kwon et al. (2007) put a strong emphasis on the risk assessment process and stated that this process must be conducted annually, and related remedial measures are required to be applied, observed and documented in the risk register. Furthermore, a formal reporting mechanism must be established for employees or internal stakeholders so that they can determine and share potential risks present in the environment that could impact the organisation (Shedden et al., 2011). Most of the time, managers along with employees might have some critical information about the risk that risk assessment is not aware of (Tipton and Krause, 2007; Da Veiga and Eloff, 2010; Shedden et al., 2011).

Unavoidably, when organisations follow the process properly, there is a higher chance that they will discover gaps in the information security controls which can be due to poor implementation of controls or the risk identification process might have flaws in it (Tipton and Krause, 2007). Phase 2 of the cycle will facilitate the management to process and re-evaluate those gaps for better controls (Shedden et al., 2011). In addition to this, the same technique, according to Brecht and Nowey (2013), also applies to exceptions and exception handling. If process owners are unable to follow policy, a risk assessment examining the potential consequences of non-compliance can be undertaken (Boehm et al., 2019). The complete procedure will eventually result in a higher-quality, more consistent exception management method (Hoffmann et al., 2020). Hence, with all five phases and better monitoring and compliance-related activities chances of major issues and possible events unnoticed decrease substantially (Woolward, 2017). The last phase helps the management in creating numerous opportunities for employees where they can raise and identified and issues, and notify the management (Tipton and Krause, 2007).

2.16.6 Fraud Triangle Theory, Motivation and Cybersecurity

Recent years have seen a significant rise in fraud, which has an impact on both client interests and financial institutions' interests (Aghghaleh and Mohamed, 2014). According to a PWC study (Tohme et al., 2015), 30% of the organisations they studied had already experienced fraud. Additionally, 80% of their fraud was carried out by employees of the companies, particularly in administrative fields like operations, accounting, and sales, and at the management level, not to mention the reliance on customer service (Owusu et al., 2021). According to Said et al., (2017), such fraud cases within the company are a great concern among cybersecurity experts. The term "fraud-related activities" refers to a variety of abnormalities and illegal acts undertaken by fraudsters that are typically unknown within a firm (Tipton and Krause, 2007). Most abnormalities found are a result of a lack of internal control measures, and in such cases, con artists perpetrate fraud by taking advantage of the loopholes (Mansor and Abdullahi, 2015). Internal dangers, including corruption, the theft of assets, and false claims, among others, are regarded to be a subset of fraud (Said et al., 2017). Owusu et al. (2022, pp. 429) define fraud as, “An intentional act by one or more individuals among management, those charged with governance, employees or third parties, involving the use of deception to obtain an unjust or illegal advantage. “The inadequacy of the oversight systems in place at institutions and businesses is what makes it possible to engage in this kind of behaviour. In these situations, fraudsters use these flaws as an excuse to perpetrate fraud (Owusu et al., 2021).

Given that fraud is committed by individuals, it is inextricably linked to human behaviour. Understanding the causes of fraud, as well as the psychological and behavioural features that drive criminals to cross moral limits, may provide a new perspective on fraud detection (Owusu et al., 2021). None of these, however, solve the issue of rapid fraud detection. Instead, modern fraud detection systems depend on the use of numerous tools that do statistical and parametric analysis based on data mining methods as well as behavioural assessments (Huber, 2017). Donald Cressey's work significantly advanced fraud theory (fraud triangle). Even though Cressey did not originate the word, his idea became recognised as such, and despite being questioned by many, it remained one of the most popular fraud arguments since later scholars expanded on and developed it even more (Aghghaleh and Mohamed, 2014).

Furthermore, Cressey's theory has been included in both the Information Systems Auditor (ISA) and International Professional Practices Framework (IPPF) standards which are mostly used by internal auditors (Abdullahi and Mansor, 2018). When people are facing financial issues which they cannot share and hold specific knowledge that the financial problem they have can be resolved by violating their position (Said et al., 2017). They apply their conduct and actions in that situation which allows them to realign their ideas as they are trusted people and they are a true user of the funds and property for which

they are violating their position (Aghghaleh and Mohamed, 2014). Cressey has identified three basic elements which lead to fraud. The first is the motivation or pressure which occurs due to financial pressure. The second element is the opportunity which occurs due to internal control weaknesses and cybersecurity lacking (Huber, 2017). The third element is rationalisation or justifying the fraudulent action which is simply a mind game where the person who is conducting fraud feels comfortable with his fraudulent action and in some cases, he is considered a victim as well (Huber, 2017).

Manurung and Hadian (2013) pointed out that everyone agrees that the best way to reduce fraud through effective risk management is to prioritise prevention. Fraud can be avoided, saving time and money as recovering stolen property after it has been done so is almost impossible (Kassem and Higson, 2012). Organisations should concentrate on the source of the issue by figuring out what motivates people to commit fraud and how to interpret their behaviour to improve fraud prevention (Manurung and Hadian, 2013). The most often mentioned hypotheses in this context are Cressey's Fraud Triangle Theory and Wolf and Hermanson's Diamond Fraud Theory (Manurung and Hadian, 2013). The Fraud Diamond Theory, which is regarded as an expanded variant of the Fraud Triangle Theory, incorporates capacity alongside the three already-known vertex types (Sujeewa et al., 2018).

Although pressure, opportunity, and justification are cohesive, it is unlikely that anyone will commit fraud unless they can do so. In other words, the deception must be capable of being committed by the potential offender (Mansor, 2015). The motivation behind this phenomenon has been explained by several fraud ideas. The assessment of all the linked variables will depend on the data utilised for the study, whether it be public or private data, and the Fraud Triangle Theory and Fraud Diamond Theory can be used to detect the probability of corporate fraud (Homer, 20200).

2.16.7 Motivation to Fraud

The components of the fraud triangle overlap; for instance, a thoroughly systematised justification may serve as someone's motivation and justify their fraudulent thinking and subsequent actions (Probst et al., 2010). The literature frequently breaks down motivation into its sub-elements, incentive and pressure, as the third piece of the Fraud Triangle (Blackwood-Brown, Levy and D'Arcy, 2021). A white-collar felon frequently combines several Deception Triangle aspects or sub-elements (Kshetri, 2013). For instance, our empirical study with high-profile scammers from Germany and Austria shows that an existing opportunity might serve as a motivation for deception (Nicholas, 2013). Opportunity and motivation, in the opinion of Meyers, Powers and Faissol, (2009), are inextricably linked, and any viable concept of white-collar crime should take this into account.

However, it is impossible to disregard the wide range of motivational factors for deception (Nicholas, 2013). White-collar crime is frequently attributed, in more populist media, to factors other

than an individual's drive for money (De Kimpe et al., 2022). Although there is an incentive for financial gain (Blackwood-Brown, Levy and D'Arcy, 2021), the study findings highlight that fraud is not solely about wealth, which is more of a metaphor than an issue with significant real value (Blackwood-Brown, Levy and D'Arcy, 2021). According to Goodwin and Nicholas (2013), there would be a lot more crime in this situation if opportunity and greed led to crime in any meaningful way. This is because the opportunity is abundant and greed is a universal human motivation. A person may assert motivational dependence on both personally and organisationally determined goals in general. Goals can be altered by external conditions, and vice versa (Blackwood-Brown, Levy and D'Arcy, 2021).

Consequently, motivation may be altered to reach the desired condition, which is one reason why certain organisations with a high risk of fraud have relatively low fraud rates (De Kimpe et al., 2022). According to Kshetri (2013), who emphasises that business settings may be criminogenic, the corporation is the culprit, the technique, the place, the excuse, the opportunity, and the victim of corporate deviance. Meyers, Powers and Faissol (2009) agree with Punch when they say that since capitalist firms obey the "code of profitability," which largely supersedes morality, they are naturally criminogenic. In addition to the amorality that results from profit maximisation, the environment around a firm also promotes the growth and acceptability of corporate crime, (Probst et al., 2010), which in turn affects people.

The 'capitalism is criminogenic' approach has some drawbacks, one of which is that it does not account for enough observable variance between enterprises and industries (Blackwood-Brown, 2018). Researchers feel that business culture and situational opportunities are significant, and that security personnel are not wasting their time. As different academic results and empirical inquiry reveal, the combination of externally imposed environmental circumstances and personal fraudulent intents has a substantial influence on the scenario, which is critical while committing a crime (Blackwood-Brown, 2018). There are organised groups as well, and their motivations for committing cyberattacks varies (Blackwood-Brown, Levy and D'Arcy, 2021).

Before September 11, 2001, terrorism and organised crime were widely regarded as distinct organisations since they did not have a common driving force. For example, in the preceding debate by Fayomi et al. (2015), some commit cyberattacks for financial gain and greed, whilst others perform cyberattacks to express their political views. There has been a notable convergence between terrorism and organised crime in recent years (Kumar and Carley, 2016). According to Sharma et al. (2010), Al Qaeda has resorted to organised criminal groups for money laundering skills. Identity and immigration crime, scam and fraud operations, and the purchase of illicit weapons and counterfeit items are all antecedent crimes used by terrorist organisations to obtain funding. Furthermore, criminal groups can

develop ideologically over time. They appear to have developed ideological or religious predispositions in South Asia that urge them to attack (Kumar and Carley, 2016).

Terrorist groups have also been found to use the internet to access information on and acquire chemical, biological, and radiological weapons, increasing the potential of terrorist groups acquiring enough fissile material to construct their nuclear bomb (Kumar and Carley, 2016). Global telecommunications technology can potentially be used to launch assaults on vital infrastructure. The spread of knowledge on the internet about dual-use research has exacerbated the problem (Gandhi et al., 2011). Faheem Khalid Lodhi was convicted in July 2006 on charges involving plotting to attack Australia's national energy infrastructure in the name of violent jihad in October 2003. Furthermore, the government must defend the cyber realm. Various organisations use online to spread their political agenda. Terrorist groups' members include engineers and computer scientists (Gandhi et al., 2011), and they have been known to utilise the internet as a means for propaganda, such as the Islamic Jihadist Group, which uses the internet to publish and promote its ideological ideologies (Fayomi et al., 2015). Furthermore, such terrorist groups are using the online realm to convey vital information that may be utilised in deadly actions. As a result, government organisations must fortify their cyberspace and prohibit such group actions (Pitropakis et al., 2018).

Politically motivated hacker organisations, known as hacktivists, have also engaged in hacktivism acts such as taking down government websites and participating in information warfare (LeFebvre, 2012). Following the collision of a US military surveillance plane and a Chinese fighter in April 2001, a well-known cyberwar between Chinese and American hackers ensued (Pitropakis et al., 2018). The Honker Union of China hacked and vandalised US government websites with phrases such as "Beat-down-American-imperialism" (LeFebvre, 2012). Other recent hacktivism efforts include the 2006 defacement of Danish websites by Islamic hackers in response to disputed cartoons ridiculing the Prophet Muhammad (Meland et al., 2022) and the April 2007 denial-of-service assaults on various Estonian government websites (LeFebvre, 2012).

2.16.8 Identified Gaps in the Literature

However, significant gaps in relation to cybersecurity, as well as the digital transformation of the UAE, can be identified after analysing the existing literature. First, although, there are numerous studies (Elmrabit et al., 2015; Rosencrane, 2022) that describe the advancement of cyber threats in the UAE, little attention is paid to how these threats have impacted SMEs in Abu Dhabi after COVID-19. The literature review focuses on the general cyber threat environment without specific information on how the SMEs are affected and the attack vectors that target them during the RD phase.

Secondly, although there are papers by Ahmed and Nanath (2021) and Zarrouk et al. (2020) have discussed historical cyber incidents and their policy implications, there are little researches that look into the long-term impact of such threats and how it has affected the SME cybersecurity in the present-day digital environment. Likewise, debates regarding risk-based cybersecurity approaches are conducted in theoretical or policy perspectives (e.g., Woolward, 2017; Hoffmann et al., 2020) but are yet to be tested in the context of Abu Dhabi's SME firms.

In addition, while the COVID-19 crisis has brought the digital transformation issue to the foreground (Younies and Na, 2020; UAE Government, 2022), there remains a lack of research examining whether the recent adoption of digital platforms has led to permanent changes in SMEs' cybersecurity awareness, culture, and practices. The second of these is the lack of attention given to the ways that SMEs leverage cybersecurity beyond mere compliance, such as for the purpose of gaining competitive advantage by improving stakeholders' trust.

Finally, there is a research vacuum regarding the applicability of protection motivation theory for SMEs in Abu Dhabi particularly in relation to employee behaviour during and after the COVID-19 pandemic. These gaps point towards the importance of context-specific, post-pandemic quantitative studies relating to SMEs in Abu Dhabi to close the gap between theory and real-world application and policy relevance.

Table 2-3: Research Theoretical Framework

The Research Theoretical Framework **The Research Aim: '***To evaluate the impact and legacy of the COVID-19 related digital adoption on information security management in SMEs operating in Abu Dhabi*.' **Addressing Research Objective 1**: 'To critically evaluate the information security practices in SMEs in the wake of the COVID-19 pandemic in Abu Dhabi.' **And Research Objective 2**: 'To conceptualise the information security challenges in SMEs in the wake of the COVID-19 pandemic in Abu Dhabi.'		
Sub Theme Heading	**Key Contributory Author(s) and Debate Highlights**	**Constructs/ Measures Extracted from the Literature**
Theme 1: Cybersecurity Landscape in the UAE: Challenges and Threats		
Emerging Threats and Attack Vectors in the UAE	Elmrabit et al., 2015; LeFebvre, 2012; Rosencrane, 2022; Grassegger and Nedbal, 2021; Bakdash et al., 2018.	• Evolving nature of cybersecurity threats specific to the UAE. • Recent trends in cyberattacks targeting organisations and individuals in the region. • The techniques and tactics employed by cybercriminals to exploit vulnerabilities.
Vulnerabilities and Weaknesses in Information Security	Miloslavskaya and Tolstoy, 2019; Barnard, 2016; Sadaqat, 2021; Zawya, 2022; Shepherd, 2022.	• Vulnerabilities in the technological infrastructure of the UAE. • Potential weaknesses in information security practices adopted by organisations. • Human error and social engineering on information security in the UAE.
Historical Perspective: Lessons from Past Cyberattacks	Ahmed and Nanath, 2021; Hakmeh, 2017; Kaspersky Lab report, 2015; Clarke,2021; OECD, 2021; Zarrouk et al., 2020.	• Historical overview of significant cyberattacks that have targeted the UAE. • The strategies used in past attacks and the subsequent cybersecurity measures implemented. • Historical incidents to inform current cybersecurity practices and policies.

Theme 2: Digital Transformation during COVID-19 in the UAE: Impact on SMEs		
Rapid Digital Adoption and Cybersecurity Implications	Younies and Na, 2020; UAE Government, 2022; Rajan, et al., 2017; Al Antali, 2018; Alketbi, Nasir and Talib, 2018; Younies and Al-Tawil, 2020	• The accelerated digital transformation initiatives undertaken by SMEs in the UAE during the COVID-19 pandemic. • The challenges and vulnerabilities introduced by the rapid adoption of digital technologies. • The impact of increased reliance on remote work, online communication, and digital platforms on information security.
Cybersecurity Landscape Amidst the Pandemic	Sena and Bhaumik, 2021; Pinto, 2016; ACM Digital Library, 2017; Atoum, Otoom and Ali, 2014; Hudson, 2016	• The COVID-19 pandemic has influenced the overall cybersecurity landscape in the UAE. • The specific cybersecurity challenges that emerged as a result of the shift to digital operations during the pandemic. • Changes in the frequency and nature of cyber threats targeting SMEs during the COVID-19 period.
Policy Responses and Information Security Practices	Gourisetti et al., 2017; Tully and Mohanraj, 2017; Rea-Guaman et al., 2018	• The UAE government and regulatory bodies responded to the increased cybersecurity challenges during the pandemic. • The policies, guidelines, and regulatory measures implemented to enhance information security in SMEs. • The information security practices adopted by SMEs in response to the unique challenges posed by the digital transformation during COVID-19.

Theme 3: Cybersecurity Culture and Practices in Abu Dhabi SMEs		
Cultivating Cybersecurity Awareness and Education in SMEs	Lanz and Sussman, 2020; Davis and Pipikaite, 2020; Tully and Mohanraj, 2017	• The level of cybersecurity awareness among employees and leadership in Abu Dhabi SMEs. • The initiatives, training programmes, and workshops aimed at enhancing cybersecurity knowledge within SMEs. • The role of continuous education in fostering a cybersecurity-conscious culture among SMEs in Abu Dhabi.
Organisational Cybersecurity Practices and Compliance	Davis and Pipikaite, 2020; Babbs, 2020; Cusmano and Raes, 2020; The National, 2021	• The cybersecurity practices implemented by SMEs in Abu Dhabi, considering industry standards and best practices. • The level of compliance with cybersecurity regulations and policies in the SME sector. • The challenges and successes experienced by SMEs in aligning their practices with established cybersecurity frameworks.
Cybersecurity Culture as a Competitive Advantage	Nuseir, 2018; Hakmeh, 2017; CSIS, 2022; Fawcett, 2020	• A strong cybersecurity culture can contribute to the overall competitiveness of SMEs in Abu Dhabi. • The integration of cybersecurity considerations into the overall business strategy and decision-making processes. • The impact of a robust cybersecurity culture on customer trust, stakeholder relationships, and the resilience of SMEs against cyber threats.

Theme 4: Theoretical Perspectives and Approaches to Cybersecurity		
Behavioural Theories in Cybersecurity Decision-Making	Wu, 2020; Sun and Shen, 2020; Kothe et al., 2019; Krishnan and Bhada, 2020; Digioia et al., 2012; Chin et al., 2012	• The application of behavioural theories, such as the Protection Motivation Theory (PMT), in understanding how individuals make cybersecurity decisions. • The psychological factors that influence motivation, perception of threats, and the adoption of secure behaviours in organisational settings. • The implications of behavioural theories for designing effective cybersecurity awareness programmes and interventions.
Risk Management Theories and Cybersecurity Strategies	Woolward, 2017; Hoffmann et al., 2020; Hoffmann et al., 2020; Paraskevas, 2020; Whitman and Mattord, 2021	• Risk management theories, including those outlined in standards like ISO/IEC 27001 and the NIST Cybersecurity Framework. • How organisations can use a risk-based approach to cybersecurity to identify, assess, and mitigate potential threats. • The integration of risk management principles into organisational cybersecurity strategies, with a focus on proactive and adaptive measures.

Source: Self-made

2.17 Conceptual Framework

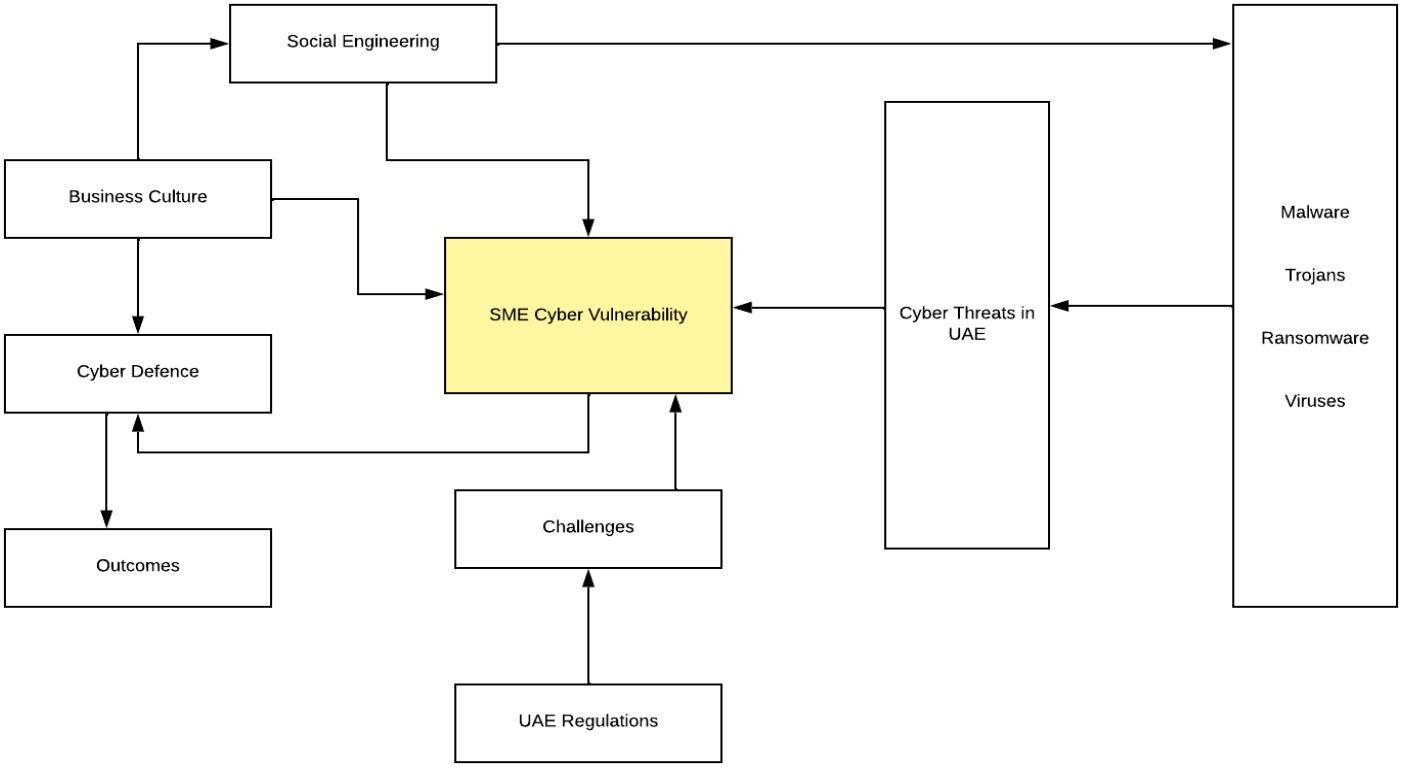

Figure 2-10: Conceptual Framework (Source: Author created)

As the figure 2-10 above indicates, social engineering is one of the major attacks that leads to Malware, Trojans, Ransomware, and Viruses. Because of a lack of awareness and potential human error chances, employees are becoming vulnerable to social engineering attacks and ultimately such lack of awareness compromised SME cybersecurity and make it vulnerable. Furthermore, the business culture is another important factor. If business culture takes cybersecurity for granted, it will eventually make cyberspace vulnerable. Furthermore, inappropriate culture and values towards cybersecurity will pave the way for social engineering attacks as well.

However, if business culture gives importance to cybersecurity despite it is not a revenue-generating function, cyber defence will be strengthened. Hence, the outcome will be better trust among customers, financial losses will be minimised, and operations will remain interrupted. Furthermore, if UAE regulations are not comprehensive enough towards cybersecurity, it will create challenges for the cybersecurity domain. Most policies must be enforced so that SMEs can comply with them for cybersecurity in a better way. However, ineffective government regulations will eventually make SMEs' cyber world vulnerable.

2.18 Conclusion

This chapter has indicated that threats to the cyber world are numerous. Particularly with the increasing rate of digital adoption, cyber threats are increasing at a rapid pace. Social engineering attacks, malware attacks, DOS attacks and various other targeted attacks have led to significant financial losses, operation disruptions and losing customer trust are notable issues and problems. Particularly, SMEs are more vulnerable as they have limited financial resources to develop robust infrastructure and lack human resources which can handle complex cybersecurity operations.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

This chapter discusses the research methodologies employed to address the study's objective of investigating the impact of COVID-19 related digital adoption on ISM in SMEs in Abu Dhabi. It specifically describes the chosen research approaches (research philosophy, strategy and data collection techniques). The chapter also looks at and briefly mentions other approaches that were considered but rejected, to provide a clear indication of the reasons for the selection of the chosen methods. Identifying and diving further into the research methodologies is the primary focus of the chapter that is devoted to this study. According to Pandey and Pandey (2021), the discussion that surrounds the precise processes that are selected and used when doing research is what is meant to be referred to by the phrase "research methodology." It is possible to apply research methodologies in order to carefully approach the study topic (Hair, Page and Brunsveld, 2019). One way to look at it is as a branch of science that explores the processes involved in doing scientific research (Sreejesh, Mohapatra and Anusree, 2014). In it, researchers examine different ways that they often use to analyse the obstacles that they face in their study, as well as the arguments for using such methods (Antwi and Hamza, 2015). In addition, it is essential for researchers to have a solid understanding of the presumptions that underpin the different methods as well as the criteria by which they may choose the methodologies and processes that are most appropriate for a given set of issues (Hair et al., 2007). All of this points to the fact that the researcher has to tailor their approach specifically to the topic at hand since there is a possibility that each issue is unique. In this respect, this chapter examines the research philosophy, research methodology, strategy, sample size and population, as well as techniques for the collecting of data and analysis of that data.

3.2 The research problem

COVID-19 restrictions forced SMEs to embrace sophisticated technologies to mitigate the impact of lockdown on business continuity. However, their preparedness to go digital was negligible and many firms were hesitant to go for digital transition, despite the urgency of technological upgrade (Shouk and Eraqi, 2015). This resulted due to poor human capital, less resources, and fear of information security hazards of implementing such technologies. SMEs had weak safeguarding measures implemented, as they were not well informed and had limited resources to invest in their protection; thus, their systems were easily exposed to cyber threats (Shouk and Eraqi, 2015; Lin et al., 2019). This research seeks to fill this gap by examining the "effect of post-COVID digital transformation on ISM in SMEs of Abu Dhabi," with a view to identifying the information security issues and the practises that should be followed by the SMEs, as well as the possible solutions to these issues. Considering the context of sociocultural and economic development of Abu Dhabi, the approach of interpretivism and qualitative research is valuable

to analyse the perceptions and experiences of SMEs in this area. By adopting these methodologies, this study ensures that the identified research problem is solved while providing an understanding of individual and organisational views and making a theoretical and practical contribution to information security management.

3.3 Personal Experience

When the researcher attempted to review the studies, it is realised that many studies (Shouk and Eraqi, 2015; Lin, et al., 2019; Costa and Castr, 2021) have discussed digitalisation during the period of COVID-19, but there is a necessity to conduct an in-depth analysis of the Information Security Management (ISM) practises and techniques used by SMEs in Abu Dhabi to evaluate the city's cybersecurity precautions and problems. Doing so will make it easier for smaller businesses to deal with similar problems in the future when they are faced with them. In addition, SMEs in other parts of the UAE can implement similar measures and solutions to handle the cybersecurity concerns that ISM is facing, which will ultimately result in an improvement in the organisation's overall performance. For conducting the research, it is necessary to decide on the research philosophy to be adopted for the study. Therefore, the next section discusses the research philosophies and paradigms.

Living in Abu Dhabi, the researcher feel the deep understanding of local business culture and norms has really helped to a great extent in framing the interviews and interactions with the representatives of SMEs. This local knowledge contributed toward elaboration on questions relevant to the specific challenges being faced by businesses here and thus allowed more insightful responses that may not have been evoked without such background knowledge.

Perhaps my status as a female and a local predetermined the level of openness and even the trustworthiness of the interviewees in such a culturally rich and diverse environment as Abu Dhabi. Being a female researcher may have encouraged a different level of candour, or perhaps provided a less intimidating environment for respondents, especially female participants or those from backgrounds where mixed-gender interactions are regulated differently.

Abu Dhabi being a city with numerous languages spoken the interviews needed consideration of language use. The researcher easily adapted and used (English) language to match that of the interviewee to make the conversation easy. This probably has implications for the richness and accuracy of the data collected.

Hailing from Abu Dhabi helped me bring an insider's perspective into the analysis of data, intuitively understanding some of the subtle local business practices and societal norms that may affect ISM practices. Locally informed insight is important for interpreting how businesses adapt to challenges around digitalisation and cybersecurity within a contextually bound culture.

Being a female researcher, the researcher brought a different kind of perspective into analysing how gender dynamics within Abu Dhabi business environments could affect ISM practices. It was very important to understand just how women can take part in and contribute toward cybersecurity for SMEs-a critical angle often missed in other broader cybersecurity research.

While this background has certainly provided many valuable insights, it has also been important to be vigilant against the potential biases. A reflexive journal in which the researcher was writing down personal experiences, as well as how these may have influenced the research process, helped to systematically bring out and address any biases.

3.3.1 Researcher Positionality and Bias Management

The role of the researcher was influenced by the professional experience and academic interest in the digital transformation and cybersecurity in the UAE SME sector. This contextual familiarity was a source of good information on the practise in organisations, but it also had the risk of being biassed. To address this, the researcher ensured the reflexivity approach during the study process, which involved using a field journal to document assumptions, reflections, and changing interpretations (Berger, 2015). Triangulation was also done through the comparison of different perspectives of the participants, and the finding was also checked with the documentary evidence and literature available. Moreover, participant validation (member checking) was used by providing summary interpretations to the sampled interviewees to determine accuracy. Considering the interpretivist character of the study, the researcher admitted the co-construction of meaning of the participants and the researcher, which guaranteed the analytic transparency and methodological credibility (Lincoln and Guba, 1985; Creswell, 2018).

3.4 Research Philosophy

The philosophy of research used in this study is interpretivism, which posits that reality should be viewed as subjective and determined by individual experiences. This perspective is appropriate for exploring how SME stakeholders consider and react to information security issues in the context of post-COVID digital transformation. Research philosophy features guidelines and principles based on assumptions about knowledge and reality for conducting research work (Žukauskas, Vveinhardt, and Andriukaitienė, 2018). Researchers modify their philosophical assumptions and adopt other research philosophies that lie between these two paradigms including critical realism, post-structuralism, and pragmatism (Saunders and Lewis, 2017). The chosen research philosophy for this study is interpretivism, which is mostly explained as a philosophical perspective that views reality as multi-faceted, and subjective, and independent of human beliefs or behaviour. Therefore, before discussing the selected research philosophy in detail and other philosophies precisely, it is discussed what would be the

ontological and epistemological stance for this study. Hence, the following sections discuss the different paradigms and the ontology and epistemology. The selected paradigm for this research is epistemology.

3.4.1 Epistemology

This study is epistemologically interpretivist and revolves around the subjective knowledge gained from SME stakeholders. The study uses qualitative methods, such as semi structured interviews, to capture participants' experiences and perspectives and a sufficient understanding of ISM practises in SMEs. The study of knowledge, or epistemology, includes a certain conception of what knowledge is and how it is acquired **(**Aliyu et al., 2014). Epistemology is concerned with providing a philosophical foundation for what kinds of knowledge are viable and how the researcher may ensure that they are sufficient and legitimate, according to Krumer-Nevo (2016). Epistemology in this research is concerned with gaining knowledge about the impact of digital transformation that took place during COVID-19 and the ways these transformations influence the security of information in SMEs. The researcher holds the interpretivist perspective, and the epistemology would be subject to interpretation and grounded on context. The researcher, using this paradigm, gathered information regarding the perspectives of small and medium-sized firms (SMEs) in Abu Dhabi on information security processes in the digital era affected by COVID-19 through the use of qualitative research methods such as observations, interviews, and examination of documents.

3.4.2 Ontology

According to the ontological position chosen in this study, reality is socially constructed. This fits with the interpretivist paradigm and the way SMEs' ISM practises are formed by the perceptions and opinions of individuals in the context of Abu Dhabi. Ontology is a branch or perspective of philosophy that deals with understanding reality or existence, characterised by conceptualisation of a domain or a formal representation of knowledge, specifically defining the links between different entities within a particular domain. Alharahsheh and Pius (2020) agreed that ontology is based on the presumptions made regarding the reality and through the ways people interpret the same reality (Aliyu et al., 2015). Ontology's subjective stance has been selected for this research and objectivism is not selected for the study as a paradigm because ontological objective assumptions are based on the concept that knowledge can only be gained via the observation of a phenomenon's existence (Maarouf, 2019). In light of the above discussion, the present study's ontological position was that it would remain independent from the researcher's knowledge and understanding. Hence, the subjectivism stance has been adopted because it perceives that social phenomena are created from the perceptions and actions of those social actors concerned with their existence. The present study's ontological position is subjectivism where reality is socially constructed. In this way, the impact of digital adoption on information security management was evaluated.

3.4.3 Axiology

From an axiological perspective, the study recognises the role of the researcher's values in the research process. The researcher's role in shaping the study was documented systematically with a view to maintain reflexivity and minimise bias. Axiology relates to the function of values in research. The positivist methodology of quantitative research distinguishes between facts and values (Aliyu et al., 2014). While facts are considered as objective truth, values are viewed as subjective, which may be inherently deceptive and hinders the quest of truth (Scotland, 2012). Here, the axiological presupposition is that objectivity is superior to subjectivity (Krumer-Nevo, 2016). In qualitative research, however, the researcher discloses the values and biases they bring to the study as well as the value-laden character of the data they collect (Park, Konge and Artino, 2020). Axiology examines the weight that researchers place on the various parts of study, such as participants, data, and audience (Luck, Jackson and Usher, 2006). In order to determine the legacy of digital adoption and its role in information security management can be based on opinion and attitude (Ryan, 2018), therefore, from axiology perspective, legacy of digital adoption can be identified.

3.4.4 The Episteme of Digital Adoption on IS in SMEs

Technology adoption in SMEs is a change process that is influenced by technology, organisation, and environment factors including COVID-19. From an epistemological perspective, the episteme of digital adoption concerns the creation, dissemination and usage of knowledge about digital adoption in SMEs. In the context of this research, epistemology offers the theoretical framework to capture how SMEs conceive and respond to information security risks and opportunities of digitalisation. The interpretivist approach allows the researcher to explore the perception of SME stakeholders on cybersecurity threats and how they make meanings of cybersecurity threats in a rapidly growing digital world. Using this perspective, the research investigates the effects of cultural, economic, and technological environments in Abu Dhabi on SMEs' ISM practises. Through such perceptions, the research is able to develop patterns and conclusions that can guide organisations on how to overcome the challenges associated with ISM.

3.4.5 Selected Research Philosophy (Interpretivism) and Justification

The interpretivism research philosophy features reality as a subjective matter that is formed according to the views of individuals in a research setting (Pandey, and Pandey, 2021). From the epistemological viewpoint, knowledge is subjective and contends that the researcher's viewpoint affects findings. According to Zachariadis, Scott and Barrett (2013), objective and value-free inquiry is impossible since conclusions are invariably influenced by the values and viewpoints of the researchers. As a result, there is a potential that results in the cybersecurity field might differ from reality due to the

researcher's perspective and ideals. The interpretivism school of thought allowed the researcher to view knowledge as, individual, and subjective. Kuada (2012) indicated that interpretivism emphasizes researching the details of social phenomena through developing detailed knowledge that understands the views of research participants related to specific research phenomena including small sample size. Notably, "*to critically assess the information security practices in the SMEs in the wake of COVID-19 in Abu Dhabi*" and "assessing the information security challenges in SMEs in the wake of COVID-19 specific to Abu Dhabi" are the objectives that can only be gained by having a data based on the perceptions and experiences of people working in SMEs.

However, this paradigm has some limitations as well. One of these drawbacks is that interpretivists often learn more about the activities taking place within their complex surroundings before extrapolating their findings to other people and circumstances (Chen, Shek and Bu, 2011). As a result, they often neglect to employ scientific methods to check the validity and applicability of their findings. The ontological position of interpretivism is often subjective as opposed to objective (Williams, 2000). Thus, the study's conclusions are undoubtedly influenced by the researcher's beliefs, perspectives, interpretations, cultural preferences, and cognitive processes, all of which lead to bias (Leitch et al., 2010). In the following, a brief description is provided to show why other philosophical perspectives have not been chosen for this study.

3.4.6 Rejecting Other Research Philosophies

Positivism, pragmatism, and critical realism were considered as alternative research philosophies. The focus of this study on subjective experiences made positivism, with its emphasis on the objective, unsuitable for this study. Similarly, pragmatism is based on the outcome of the practical and critical realism is based on an objective empirical approach. Therefore, these approaches were also incompatible with the emphasized context and interpretivist perspective of this study.

3.5 Research Approach

The approach of the study is inductive in which the researcher develops theories and concepts from specific observations (Bingham and Witkowsky, 2021). This approach fits with the nature of the study and helps explore the ISM challenges in SMEs. A research approach is defined as an organized plan and procedure that includes several stages and phases that enable the researcher to carry out a comprehensive process for collecting, analysing, and interpreting data gathered throughout the study. Research questions and their nature are an essential part of the research, according to the research strategy, which is akin to research philosophy (Kamal, 2019). The research strategy related to data gathering and the research approach involved with data analysis may be divided into three categories inductive, deductive and

abductive (Kovalainen and Eriksson, 2015). The selected approach for this study is inductive, and the following section details the inductive research approach and justifies selection.

3.5.1 Selected Research approach (Inductive) and justification

The inductive approach allows data collection and analysis to be flexible so that themes emerge from participants' experiences. This method is particularly suited for meeting the study's objectives, for example, developing a model for best practises in SME ISM in digital transformation. The inductive research technique entails researching while keeping in mind the research questions as well as the primary components' purposes and objectives, obviating the need for hypothesis testing in research (Ragab, and Arisha, 2018). The establishment and discussion of the new hypothesis that arises from the evidence obtained in the study are related to an inductive research technique (Alharahsheh and Pius, 2020). Given that the researcher is not required to use any predetermined information, inductive reasoning is considered flexible. Inductive research works its way from specific observations to broader conclusions. The use of inductive reasoning proved to be the most productive way to construct theories and concepts.

During the study of the information security problems that SMEs in Abu Dhabi experienced during the pandemic, the researcher used an inductive method to extrapolate general ideas or concepts from the respondents. This contributed to the construction of a conceptual framework that was used to get an understanding of the challenges that a variety of SMEs encounter (Kovalainen and Eriksson, 2015; Barnham, 2015). This method of conducting research can also be highly time-consuming at times (Walle, 2015). The inductive approach, according to Antwi and Hamza (2015), is rather a flexible approach where the researcher has the liberty to interpret the data as per his understanding.

The inductive approach is relevant in exploration (Easterby-Smith et al., 2021), the researcher in the present study explored the reality of the cyber world by evaluating the impact of COVID-19-related digital adoptions on information security management (Pandey, and Pandey, 2021).

With the assistance of the inductive method, developing new models for best practices with specific facts was made far simpler, which was the fourth objective of the study. The fourth objective of the study was, "*to critique options for addressing the SME cyber challenges with the development of an associated model for best practice*." When evaluating potential solutions to SME cyber issues, using an inductive technique assisted the researcher in synthesising the findings into a model that was representative of best practices.

To summarise, the inductive research method was an excellent choice for reaching the research objectives because it enabled the researcher to start with specific situations such as information security processes, issues, resources, and solutions, and then extrapolate to more general concepts. This made the

inductive research method an excellent choice. The inductive approach has, however, certain limitations as well that must be considered to benefit fully from it. It does not apply necessarily to broader contexts other than chosen in the research. The possibility of the inclusion of bias is always there due to the human interpretation of the collected data. This approach is also not effective in determining specific links between different variables in a given research setting.

3.5.2 Deductive and Abductive Approach

The deductive and abductive approaches were considered but were not selected for this study. As the study aimed to explore rather than test predefined theories, deductive reasoning based on hypothesis testing was deemed unsuitable (Mir, and Greenwooed, 2021). Though useful for integrating qualitative and quantitative data, abductive reasoning was too complex and time consuming for the purpose of the study.

3.6 Research Strategies

The study adopts a case study strategy, which is well-suited for exploring ISM practices in SMEs within the specific sociocultural and economic context of Abu Dhabi. The main research strategies include experiments, surveys, case studies, action research, grounded theory and archival research (Kumar, 2018). In line with the critical realism and abductive research philosophy, the current research work opts for the case study as the main research strategy (Saunders et al., 2015). The data collection was done by interviewing individuals and getting their replies to the interview questions (Mack, 2010). A representative sample of SMEs with the primary research instruments being semi-structured interviews (Glesne, 2016). However, before discussing the case study strategy, it is necessary to have an overview of the other options as well. Hence, in the following sections, different options that were available to the researcher have been discussed. However, the selected strategy for this research is a case study.

3.6.1 Case Study as a chosen research strategy

Case studies offer a detailed and contextualised understanding of phenomena, which makes them ideal for studying the ISM practises of SMEs across different industries. Semi-structured interviews augmented this study to facilitate in depth exploration of the unique challenges and solutions SMEs have faced. A case study helps the researcher grasp the occurrences in context (Hair, Page and Brunsveld, 2019). The research strategy for the case study includes an exploratory and descriptive investigation of the occurrence, the participants, or the group. Case studies provide settings in which to identify details of institutional development, distinctive qualities, parallels between cases, and other things via the thorough investigation of contemporary reality (Blumberg, Cooper and Schindler, 2014; Yin, 2011). For

the present study, the case study strategy was followed because the researcher collected data from the SMEs regardless of their industry and business model (Yin, 2011).

The case study approach allowed the researcher to understand the specific implications that the COVID-19 outbreak has had on information security needs within the context of SMEs operating in Abu Dhabi. The researcher looked at each SME's environment through the lens of a case study, taking into consideration factors such as the sector it operates in, its size, and the practices that are currently in place. This contextualisation was essential to accomplish Objective 1, which was to conduct a critical analysis of information security practises, and Objective 2, which was to conceptualise challenges within the specific sociocultural and economic environment (Hair, Page and Brunsveld, 2019).

An in-depth investigation of the tools and solutions that SMEs have selected was the third objective of the research and the case study was the suitable option. The case study strategy provided the opportunity for the researcher to conduct an in-depth investigation of the problems and solutions that SMEs have chosen (Nzekwe-Excel, 2021). One of the objectives of the study was to critique the available options and then the development of a working model that includes good practices. By utilising a case study methodology, it was feasible to analyse a variety of ways to resolve cybersecurity concerns faced by SMEs (Yin, 2011). The researcher successfully established contrasts and comparisons, discovered similarities and differences, and developed a model for best practices based on a comprehensive investigation of the unique circumstances.

Other research strategies such as ethnography, grounded theory, action research, survey and experimental research were not chosen because they could not address the objectives of the study. For example, because ethnography takes time and grounded theory depends on empirical data, they were not suitable for the research context. Likewise, survey and experimental methods were not deep enough to meet the requirements this qualitative inquiry.

The case study research design was deemed the most appropriate for this study, as it enables an evaluation of the specific issues and practises of SMEs in Abu Dhabi regarding the digital adoption and ISM in post-COVID period. This design facilitated the researcher to concentrate on identifying the real-life context of SMEs by carrying out semi-structured interviews with the 23 managers and two officers of the SMEs who were in a position to provide first-hand experience and perception. The semi-structured approach helped to be more flexible when asking about particular problems connected to ISM challenges, including the lack of resources, cybersecurity threats, and organisational preparedness, as well as allowing for the development of new ideas that enriched the study's results. For instance, interviews were designed to know how SMEs managed cybersecurity threats in the course of adopting digital technologies and to know if cultural or organisational factors affected the firms' ISM plans. The use of case studies was especially appropriate for the research objectives because it focused on the

contextual factors influencing ISM practises in SMEs and offered the richness of data to explore the details of the views, which would have been difficult in other methodologies such as surveys or experiments. The case study design of the findings made the results relevant to the sociocultural and economic context of Abu Dhabi, as well as applicable in practise, thus fulfilling the research objectives in full.

3.7 Research Choices

Sampling techniques have two major types which have been used by many researchers according to their needs and the demand of the study. The first is probability sampling and the other is non-probability sampling. In probability sampling, the researcher has given all the respondents the same chance to participate in the study, and in non-probability sampling, the researcher gives the chance to a specific group of people to participate in the study (Easterby-Smith et al., 2021). In this research study, the non-probability purposive sampling technique was used.

Purposive sampling refers to the selection of participants based on some specific characteristics that are required to collect the data relevant to the study topic and complete the research successfully (Patrick, Zou and Xu, 2023). In this type of sampling, the researcher reaches the population or sample of the population who is more relative to the study topic and has knowledge specific to the topic leading the researcher to collect the data from the respondents that can help answer the research questions. Purposive sampling allows the researcher to reach a specific audience, but it also contains some limitations such as it is difficult to generalise the results from the specific sample to the overall population (Johnson and Christensen, 2008). However, the limitation of this sampling is that it encourages the selection of only those cases that are information-rich (Gattis, 2019).

The nature of the study and the type of research were strongly linked in terms of research choices. The research study's nature may be divided into three categories. Qualitative, quantitative, or mixed research, which combines qualitative and quantitative research, are the three different aspects. According to Bairagi, and Munot, (2019), the amount of research in these many sorts of studies varies from one another, and the research technique varies depending on the study's nature. Qualitative and quantitative research methodologies, on the other hand, have distinct qualities and attributes (Jamshed, 2014).

This research study opts for a qualitative research method which was the assimilation of subjective views in the study. The qualitative research method was completely aligned with the interpretivist research philosophy. The study looked at the effects of post-COVID digital adoption on ISM in SMEs in Abu Dhabi to show the usefulness of interpretivism that led to qualitative research methods. Current research work was executed with the main focus on the implications of executing research with a qualitative research design involving the collection of qualitative data. A qualitative research design

demonstrates the features and benefits that have been associated with subjective information. According to Kumar (2018), the use of a qualitative research design enables the researcher to focus on integrating exploratory analysis addressing the problem of the research and obtaining meaningful information. By utilizing qualitative data, researchers ensure gaining in-depth knowledge (Antwi and Hamza, 2015).

3.8 Time Horizons

Time horizons are associated with the specific period that has been used for the successful completion of the research (Easterby-Smith et al., 2021). Time horizons involve two different kinds including cross-sectional and longitudinal time horizons. According to Saunders et al. (2007) longitudinal is used for research conducted for a long period and cross-sectional is used for a shorter period. This research study focuses on identifying and exploring the opinions of SMEs of Abu Dhabi related to the legacy and impact of COVID-related digital adoption on the ISM; therefore, a cross-sectional time horizon supports the objective of the study to be achieved at a single point in time.

3.9 Techniques and Procedures

The target population, sampling frame, sample size, and sampling procedure employed in this study are all included in the sampling design.

3.9.1 Population

The population of the research was based on the managers, executives, and other concerned officers from companies. This population was selected using a purposive sampling considering their seniority in roles and they could support the research with the knowledge they hold based on their roles and experiences (Patton, 2014). This selection of a sample population was done purposefully as the aim was to examine the impact of digital adoption during COVID-19 and its impact on the security management of the information. According to Creswell and Creswell (2017), researchers use purposive sampling to learn and understand the necessary aspects of the topic. To understand the research topic, challenges associated with digital adoption and solutions to resolve those challenges, the participants of the research were selected intentionally because the researcher knew that leaders, managers, and officers were experts in their field and they had topic-specific knowledge due to which they could better answer the research questions and their knowledge-based answers could help to address the research objectives.

3.9.2 Sample size

The sample size for this research includes a small population of people and can be considered as a target population. In detail, 23 executives and two officers from SMEs across Abu Dhabi were asked questions concerning their perception of digital and its relevance to SME businesses. Furthermore, two officers in SMEs were included in the sample size to make it 25 participants. About data collection procedure, interviews were conducted using semi-structured questions which included set questions

whose answers had to be guided by the respondent, and probing questions to ensure that the respondent understood the topic being discussed and to give depth to the topic under discussion. The use of follow-up questions helped in elaboration of the answers, obtaining more detailed information, and discovering other problems. The choice of using 25 participants was considered reasonable because data collection reached the level of a point where no extra themes were generated from the interviews. Data saturation on the other hand is a stage in qualitative research where the researcher fails to discover new data or issues that relate to the research question or research question. The selected sample size is satisfactory, thus proving that the collected data is sufficient in addressing the research objectives. This is in concordance with Chen and Reed (2001) who posited that a saturation test establishes the appropriateness of the sample size. This is consistent with the sample size range investigated in other comparable qualitative studies as seen from another research works (Kaur et al., 2021; Modgil et al., 2022; Ali et al., 2020). Table 3-1 also gives a breakdown of the nature of the sample in relation to the research objectives outlined earlier.

Table 3-1: Sample selected for the Study

Company (SME) Name	**No of Managers Interviewed**	**No of officers Interviewed**
Beta Information Technology Co	5	-
Eagle Eye Smart Systems	5	-
EMCC Company LLC	4	-
Hader Security & Communication Systems (HSCS)	5	-
Bin Murshed Group	4	2

The following is a summary of the research population, inclusion criteria, and sampling rationale:

Table 3-2: Inclusion Criteria and Rationale for the Sample

Category	Number of Participants	Inclusion Criteria	Sampling Rationale
Managers	23	Must be involved in strategic decision-making and/or have knowledge of ISM challenges during digital adoption.	Managers were included to gather insights into organisational policies, strategies, and challenges related to ISM, with a focus on the context of digital transformation in SMEs.
Information Officers//Technical Team Member	2	Must be directly involved in implementing ISM measures and handling digital adoption processes.	These participants were selected to provide detailed technical perspectives on how ISM processes were executed and the specific cybersecurity challenges encountered during digital adoption in SMEs.
SMEs Criteria	5	Must operate in Abu Dhabi and have undergone some degree of digital transformation during or after COVID-19.	SMEs were chosen to focus on organisations that experienced the practical implications of post-COVID digital adoption, enabling a targeted exploration of ISM practices within the specified geographical context.

3.9.3 Rationale for Sample Size and Data Saturation

In this study, 25 respondents were chosen who would represent small and medium enterprises (SMEs) owners, managers and IT specialists in Abu Dhabi. The selected sample corresponds to the accepted qualitative research principles, when the priority is given to the depth of understanding, rather than to the number of generalisability (Creswell, 2018). Research investigating information security

behaviour and digital transformation within SMEs will usually achieve thematic adequacy on 20-30 interviews (Guest et al., 2006; Saunders et al., 2018).

Saturation of data occurred after no additional themes or understanding came up during the coding and the thematic analysis processes. Following the interviews, which were about 23, common trends were found in the descriptions of cyber readiness, digital adoption and management of information security by participants. The remaining two interviews were carried out to ascertain redundancy and saturation consistency. It was decided to retain 25 participants in this way, as a compromise between theoretical adequacy, breadth of perspectives, and empirical adequacy, as well as credibility and transferability of results (Lincoln and Guba, 1985).

3.10 Data Collection

For collecting the data through interviews, the researcher had different options: structured, unstructured and semi-structured interviews. However, semi-structured interviews were selected for being suitable for this study. Structured interviews were not used because in this type of interview, the questions are predefined, and such interviews limited the data collection by restricting the researcher from asking any other question than written questions that cause to limits the knowledge (Banister et al., 2011). Further, these are close-ended interviews that limit the ability of the respondents to share their feelings and actual experiences (Mwita, 2022). On the contrary, unstructured interviews are non-directive and due to the unavailability of the predesigned questions, the researcher might not be able to collect the data required and may miss to ask important details (Lee and Herstatt, 2015).

Hence, the data collecting source for this study is primary, and semi-structured interviews were used to collect the data. The semi-structured interviews consisted of a variety of open-ended inquiries, including interrogation and probing questions. The opportunity to ask probing questions helped the researcher to clearly understand the topic and reach the objectives (Lee and Herstatt, 2015). One of the limitations of semi-structured interviews was that the data may be based on biases (Bless, Higson-Smith and Kagee, 2016).

Importantly, it is to mention that obtaining approval from the selected companies for data collection has proven to be quite difficult for the researcher, taking nearly three months to navigate.

Despite receiving ethics approval, the researcher encountered several obstacles during this process:

1. Rejections: Some companies ultimately declined to participate and some other declined after initially showing interest. Additionally, one company was found to be closed and no longer exists.
2. Location Constraints: With two companies whose Chief Executive Officer (CEOs) were supportive and willing to help, it was confirmed that they operate solely from Dubai and do not have offices in Abu

Dhabi. Unfortunately, this disqualified them from participating in the current study, as this research requires the inclusion of companies with a presence in Abu Dhabi.

3. Ethics Revisions: The researcher had to update the ethical forms several times to include new companies and secure additional ethics approvals.

4. Interview Timing: One interview had to be conducted late at night, at 10 PM, due to scheduling conflicts.

5. Client Communication Issues: In two instances where the researcher had secured both ethics and company approvals, certain challenges were confronted. One client kept the researcher waiting in an online meeting for an hour without response. Another provided generic and uninformative responses, primarily citing confidentiality, which hindered the researcher's ability to gather essential details. Moreover, the researcher was not granted permission to interact with other employees within the company.

These experiences highlight the complexities involved in engaging corporate entities for research purposes.

Since the population of Abu Dhabi is linguistically and culturally diverse, language and cultural issues were carefully handled during the interviews. All interviews were conducted either in English or Arabic to meet the participant's preference and to minimise confusion. The researcher had prior knowledge of the business practises in the Middle Eastern countries and also has a good understanding of Arabic language which allowed the participants to express themselves with ease. Also, a brief orientation was provided to participants prior to commencement of the interviews sessions to recall the study's purpose, scope, and implications and develop a friendly rapport between the interviewee and the researcher so that the participants did not feel intimidated, especially when the participants had no exposure to academic research. This format was especially beneficial because the researcher was able to probe for predetermined topics, while still being able to respond to new ideas. This flexibility was essential to capture the richness and variety of ISM practises in SMEs of various industries in Abu Dhabi.

3.10.1 Participant Recruitment and Sector Representation

A purposive sampling technique was used to recruit participants, and they were SME decision-makers who had an active digital operations or information security management. The invitations were sent via the Abu Dhabi Chamber of Commerce contacts, professional LinkedIn groups, and the available SME business associations. The inclusion criteria included that the participants (1) have to be in operation in Abu Dhabi (2) with the number of staff ranging between 10 and 250 (3) and (4) has implemented at least one type of digital technology (cloud computing, ERP, or e-commerce platforms) after the COVID-19 pandemic.

The 25 SMEs were of various economic sectors such as retail, logistics, construction and education, healthcare and information technology. This diversity has guaranteed sectoral equilibrium and given a chance to compare mature and emerging businesses that are digitally mature. The recruiting procedure was based on voluntary involvement and flexibility to adapt to the availability and privacy concerns of the participants.

3.11 Evaluation of Research Design Quality

It is important to assure the quality of the research design in order to build credibility of the research and its results. This section evaluates the design's quality through key metrics: Construct validity, internal validity, external validity and reliability. By addressing these aspects, the study proves its applicability and offers a basis for evaluating the trustworthiness of its results.

3.11.1 Construct Validity

Validity indicates the measurement of what the research process is intending to measure, and construct validity is an aspect of validity (Piedmont, 2024). In the current study, the interview questions were developed in such a way that they were consistent with the research questions. Every question was created to capture the perception of the researcher regarding certain aspects of ISM and digital transformation in SMEs. For example, questions that asked about cybersecurity threats, available resources, and organisational preparedness, matched the research objectives. The development of the interview guide was an iterative process, and before administering interviews for the main study, a pilot test was conducted with a selection of participants to cheque for understanding and the applicability of the questions. In this way, the construct validity was maintained due to the close connection between the questions and the goals of the study.

3.11.2 Internal Validity

Internal validity relates to the extent to which the study achieves the objective of measuring the relations and phenomena of interest (Sargeant, Brennan and O'Connor, 2022). The thematic analysis was used to make the representation of the data as authentic and contextualised in the participants' responses as possible. All interviews were transcribed in detail, and the texts were analysed without any preconceptions of the researcher. Peer-reviewed literature was used to cross-cheque codes with the study, so that emerged themes were both data- and theory-based. For instance, the patterns like the effects of resource constraints on ISM practises were revealed in various SMEs, which indicates the reliability of patterns within the dataset.

3.11.3 External Validity

External validity refers to the question of how far each finding of the study is applicable in cases other than that in which the study was conducted (Egami and Hartman, 2023). With regard to the interpretivist philosophy and the fact that the study is qualitative, the research does not seek generalisability in the conventional manner. However, it puts stress on transferability, which is attained by providing detailed contextual information and descriptions of the participants. For example, the study presents rich descriptions of cultural and economic contingencies of SMEs in Abu Dhabi which allows the reader to judge the transferability of the findings. Although the study is contextualised, the process of contextualisation is detailed, ensuring that the findings are useful to other SMEs experiencing similar issues.

3.11.4 Reliability

Reliability means the consistency of procedures used in research or stability of the generated results (Vu, 2021). To improve the reliability in this study, a semi-structured interview guide was developed and followed while the analysis was done systematically. Inter-code reliability was maintained through multiple cycles of coding in which the initial codes were checked to guarantee that they captured the details of the data set appropriately. Validity was also impacted by peer review of selected transcripts and themes that reduced bias in the interpretation of results. Furthermore, all the processes of data transcription and analysis, including theme development, were effectively saved, making the study replicable in the same conditions by other researchers.

3.11.5 Comparison with Other Similar Research

To enhance the quality of the research design, the results and approaches of the study were benchmarked against those used in other ISM studies and research on digital adoption. For instance, Ali et al. (2020) as well as Modgil et al. (2022) used qualitative approaches to analyse cybersecurity threats in SMEs and gathered data contextual information to provide insights in organisational behaviour. These studies also employed the semi-structured interviews and thematic analysis, which supported the suitability of the chosen approach to ISM practises. The fact that the results are similar to previous research, for example, the importance of resources and their availability for cybersecurity practises, proves the reliability and applicability of the current research methodology.

3.12 Data Analysis

Thematic analysis was used to examine the qualitative data gathered during the interviews. Thematic analysis is a sort of analysis that involves extracting themes from raw data (Bairagi, and Munot, 2019) in order to help the study's goal of creating a hypothesis based on the findings. The flexibility of conducting semi-structured interviews, as well as the adaptability of qualitative research techniques,

allows researchers to tailor the data analysis to their own goals. This approach proved effective because qualitative studies have examined attitudes, opinions, beliefs, and experiences that can be classified (Garner and Scott, 2013).

The basic thematic analysis includes the following steps. Researchers can execute forward and backwards through these steps (Howitt, 2019):

i. Text Material Transcription: Any type of text material can be used. In this project, Interviews were transcribed using notes and written documentation.

ii. Analytical attempt: The work done by the researcher to arrive at the final themes includes the following elements:

- Learning the data so that the researcher is becomes familiar with it.
- Coding and conception in great detail.
- The level to which the researcher is able to utilise the data in order to ensure that the analysis is as close to the data as possible.
- The scope of the issues and the efforts made to resolve them.
- The frequency and depth with which the researcher compares and contrasts data and analyses.

iii. Determine main and sub-themes: Because various researchers may uncover a varied number of themes, it is critical that the researcher clearly demonstrate how the themes were developed during the study (Howitt, 2019).

Though thematic analysis is beneficial in summarising the outcomes by converting the data into meaningful themes and discussing them, it has some limitations such as ensuring the reliability and validity of the data is challenging in thematic analysis (Kishore, 2023).

The data analysis involved thematic analysis, based on the model proposed by Braun and Clarke (2012). First, verbatim transcripts of digitally recorded interviews were made to capture all of the content, including nuances and context, essential features in qualitative analyses. These transcriptions were checked carefully against the playback of recordings to make sure it is what was said. The actual data cleaning began after transcription by excluding those redundant or off-topic sections that did not contribute to the answering of the research questions. This involved removing all filler words and conversational fluff that would detract from the key substance. Personally identifiable information was anonymized to protect the confidentiality of the participants and for the sake of ethical research standards.

The researcher reviewed the cleaned transcripts multiples times to immerse myself in the data, which helped the researcher understand the depth and breadth of the content discussed during the interviews. This step of immersion was crucial in identifying preliminary patterns and insights. Initial codes were

developed. The process of coding was iterative in that while themes started to emerge, some of the initial codes were combined, split, or discarded depending on how relevant they were to patterns that were beginning to emerge. Data were continuously compared with the rest of the data to develop codes and also maintained consistency. Such comparisons formed salient features while assessing the complexity and depth of data, thereby leading to the emergence of robust thematic constructs.

Potential themes were identified from the refined codes. These themes were then reviewed in detail to determine whether they related directly to the study objectives and whether the interviews were comprehensively represented. Themes were reviewed primarily for coherence. A theme was checked if it best reflected compiled codes and allowed the making of a meaningful contribution to overall research questions. The adjustments were made by splitting, combining, or even redefining themes to be well-developed and supported by the data.

In order to add weight to the analysis, the findings from the interviews have been compared with existing literature. This iterative refinement ensured that these themes not only reflect the data but also are robust enough to stand external scrutiny.

The finalized themes led to structure the findings section of the study, each with their supporting quotes from participants and integrated with insights from the literature in order to gain a full understanding of the impacts of COVID-19 on ISM within SMEs.

3.12.1 Thematic Analysis and Theoretical Alignment

Thematic analysis was used in analysis because it is consistent with the theoretical underpinning of the study in Protection Motivation Theory (PMT). PMT offers a behavioural model of how people perceive the severity and vulnerability of cyber threats and weigh their coping potential (response efficacy and self-efficacy) in dealing with information security threat (Rogers, 1983). Systematic data identification and interpretation in the presence of these PMT constructs were supported by the thematic analysis. In accordance with the six stages of the process introduced by Braun and Clarke (2006), the initial codes were inductively derived based on the information and further refined and deductively projected onto PMT dimensions to promote theoretical consistency. This two-fold analytical approach allowed the development of context-dependent insights and did not lose the consistency with the cognitive and motivational framework of PMT. Thus, thematic analysis acted as a descriptive and interpretive tool, connecting the experiences of the participants with the conceptual framework of the study the SME information security behaviour.

3.12.2 Ensuring Coding Reliability

Reliability in qualitative coding was ensured through multiple verification strategies. The researcher developed a detailed codebook during the first cycle of coding to maintain consistency in interpreting and categorising the interview data. Each initial code was clearly defined with inclusion and exclusion criteria to ensure uniform understanding throughout the analysis. To enhance the dependability of interpretations, peer debriefing was conducted with two academic colleagues familiar with thematic analysis, who reviewed a sample of coded transcripts and provided feedback on theme clarity and consistency.

Discrepancies were discussed and reconciled through iterative comparison, strengthening the coherence between data segments and emerging themes. All coding decisions were documented within NVivo 12, ensuring an **audit trail** of the analytic process. This systematic approach increased both the reliability and confirmability of the thematic analysis, aligning with Braun and Clarke's (2021) reflexive principles emphasis on analytical transparency in qualitative research.

3.13 Legal / Organisational Considerations

The regulatory framework that controls research, such as the General Data privacy Regulation (GDPR) of 2018, provides a significant boost to the participants' and researchers' ability to maintain their confidentiality during the study process. Since University of Lancashire is located in the United Kingdom, the General Data Protection Regulation (GDPR) is an applicable regulatory framework that controls research practises. The process for the study needs to be in accordance with specific legal requirements in order to safeguard the participants' rights and their right to privacy.

Autonomy of the Participants: General Data Privacy Regulation (GDPR) says that data should be collected with the consent of participants. While conducting a research study, researchers are required to ensure the respect of the research participants. This includes participants possessing the authority to participate in the process of research, whether participants are willing to participate in specific processes, share specific experiences and also have authority to withdraw from the research process without influencing the rights of the participants. Moreover, incomprehensible explanations, inadequate information, and different external stress are some factors that could result in influence the decision making of the participants. It is important for the research to assure the minimal influence of these factors on the autonomy of the research participants (European Data Protection Supervisor, 2020). It will not only give the respondents confidence, but the researcher will also be able to ensure that the responses will be accurate and based on the true experience of respondents.

Principle of no harm: It is important for researchers to execute the research on the basis of improving the well-being of participants, associated communities and as a whole entire society also involve in this

specific principle. Each process of research possesses some potential benefits and harms. Therefore, it is important for the research to make efforts for reducing the probability that research influenced research influenced the participants. Moreover, the researcher should make efforts to increase the interest levels of the participants and should emphasize the well-being of the entire society by advancing the existing knowledge base. Using this principle, the researcher communicated the rights to withdraw, confidentiality and anonymity of the data. The researcher has been responsible for developing a proper mechanism to seek the approval based on the communicated information (European Data Protection Supervisor, 2020).

Principle of Justice: The principles of justice involve the responsibility of research to treat the associated stakeholders with fair and equal means. It involves treating all existing and potential stakeholders of the research with equal respect. Moreover, the researcher should emphasize assuring the development of understanding with participants, understanding their views and identifying those patterns from their opinions that completely portray their authentic views. Using this principle, the researcher treated all participants fairly and provided them with equal chances of flexibility (European Data Protection Supervisor, 2020).

3.14 Addressing Ethics and Risks of the Study

While carrying out this research, collecting data related to ISM practices among SMEs, it was essential to ensure fulfilment of ethical considerations and risk management measures. This section will elaborate on the ethical standards adhered to during the research process and discuss the potential risks for the study, as well as the measures that were taken to avert them.

The consent of all participants was sought in advance of interviews, with information provided on the purpose of the study, the nature of their involvement, and their rights vis-à-vis the research, such as the right to withdraw at any time without consequence. Participants were assured that all information provided would be treated as confidential communications and private, and that the identity of no participant would appear in reports or any other outputs from this research.

In order to maintain participants' privacy, all the identifying information was removed or changed in the transcriptions and any published material. Data were stored in a secure environment, and access was limited only to the researcher only. This was crucial because the nature of the discussion could involve sensitive topics regarding ISM practices and potential vulnerabilities of their organisation.

Transparency and honesty were ensured from the start of the research process to the end; i.e., on the purpose of the study and on the use of the data collected. Such openness helps build the confidence of the participants, by maintaining that research was performed without a violation of integrity in the information provided.

Cybersecurity good practices being discussed in this study were of a sensitive nature; hence, there was a risk that confidentiality could be inadvertently breached. Stringent protocols in data handling were established to reduce the occurrence of this risk. Data were encrypted and stored in secure password-protected databases. Only anonymized data were used when analysing or processing data.

Since the very beginning of this research project, throughout the study process, it required consideration concerning ethical standards. The activities performed in research were evaluated recurrently according to the provided ethical guidelines. The research might have involved discussions about cybersecurity failure or breach that may cause distress or discomfort for participants. Due to the sensitive nature of the discussion, the informed consent form indicated the possibility of emotional harm. The participant was also reminded during an interview of their right to refuse to answer certain questions or stop being interviewed anytime. Support resources were provided to the participants for their respective concerns related to the study.

Ethical approval for the study was obtained from the University of Lancashire's Research Ethics Committee. Beyond informed consent, several measures were implemented to protect participants' rights and data integrity. All participants were provided with an information sheet outlining the study purpose, voluntary nature of participation, and right to withdraw at any time without consequence. Each participant signed a written consent form before the interview. To ensure anonymity and confidentiality, participant identifiers were replaced with alphanumeric codes (e.g., SME1–SME25) in transcripts and analysis. Any information that could reveal organisational identity was omitted from quotations. Interview recordings and transcripts were stored securely on a password-protected university drive, accessible only to the researcher and supervisory team. Data will be retained for five years after publication in accordance with UCLan ethical policy, after which all files will be permanently deleted. These measures collectively ensured compliance with the General Data Protection Regulation (GDPR, 2018) and upheld ethical principles of beneficence, autonomy, and confidentiality (Creswell, 2018; BERA, 2022).

3.15 Summary

This chapter has described the research methodology used to realise the study goal, which was to examine the effect of COVID-related digital adoption on ISM in SMEs in Abu Dhabi. The researcher adopted an interpretivist research paradigm owing to its view that knowledge is constructed and situated. This approach was in line with the study objectives of obtaining the SME stakeholders' insightful perceptions on ISM challenges. In this study, data was collected through semi-structured interviews with managers and executives from five SMEs in Abu Dhabi; adopting the inductive research methodology. The purposive sampling technique made certain that only participants with the necessary expertise and

experience were selected. Structuring of the data was done by means of an interview guideline that aimed at generating detailed, context related answers to the research questions; the analysis of the qualitative data was done by means of thematic analysis in order to get to the core of the research questions and identify the important themes. Through the use of qualitative research techniques, the study was able to uncover the antecedents and dynamics of digital adoption and ISM in SMEs, providing insights that are both meaningful and useful in practise. The discussions in this chapter provide a rich background for the research design and corroborates the suitability of the design in fulfilling the study goals and objectives and makes a useful contribution to the existing body of knowledge on cybersecurity and digital transformation in SMEs.

CHAPTER 4: DATA ANALYSIS

4.1 Chapter Introduction

The analysis of primary data collected presented in this chapter is critical to understand the deep implications of COVID-19-induced digital adoption on Information Security Management in SMEs of Abu Dhabi. This research undertakes the unravelling of the complexities that post-COVID digital adoption has created and how it is evident in ISM among the SMEs in Abu Dhabi. Emphasis is laid here on a detailed study of the challenges with information security the sector suffers from, alongside the pragmatic practices and solutions that can come close to fortifying the cyber defences for them. The study provides stakeholders with actionable insights based on the analysis findings, with which they may be able to take transformative strides toward information security resilience in the face of the relentless march of digital evolution.

4.2 Thematic Analysis

An iterative process of thematic analysis was conducted, which ensued assurance for the integrity and credibility of the data interpretation. Central to this task was iterative theme refinement using a reflexive stance to avoid presuppositions and bias.

Table 4-1: Participants Codes and Experience Level

Sr. #	Participant's Job Role	Participants Codes	Experience Level (in years)
1	Senior Manager	P01	17
2	Senior Manager	P02	25
3	First Line Manager	P03	5
4	First Line Manager	P04	20
5	First Line Manager	P05	22
6	Technical Team Member	P06	4
7	First Line Manager	P07	5
8	First Line Manager	P08	12
9	First Line Manager	P09	8
10	Technical Team Member	P10	10
11	Senior Manager	P11	10
12	Senior Manager	P12	8
13	First Line Manager	P13	21
14	Senior Manager	P14	23

15	First Line Manager	P15	8
16	First Line Manager	P16	22
17	First Line Manager	P17	20
18	First Line Manager	P18	18
19	Senior Manager	P19	18
20	First Line Manager	P20	4
21	Senior Manager	P21	10
22	First Line Manager	P22	5
23	First Line Manager	P23	5
24	First Line Manager HR Recruiter	P24	5
25	First Line Manager	P25	5

Once the interview transcripts were anonymised, the data analysis process was started.

The following figure depicts the data analysis process as per the rules of the thematic analysis posited by Braun and Clarke (2012).

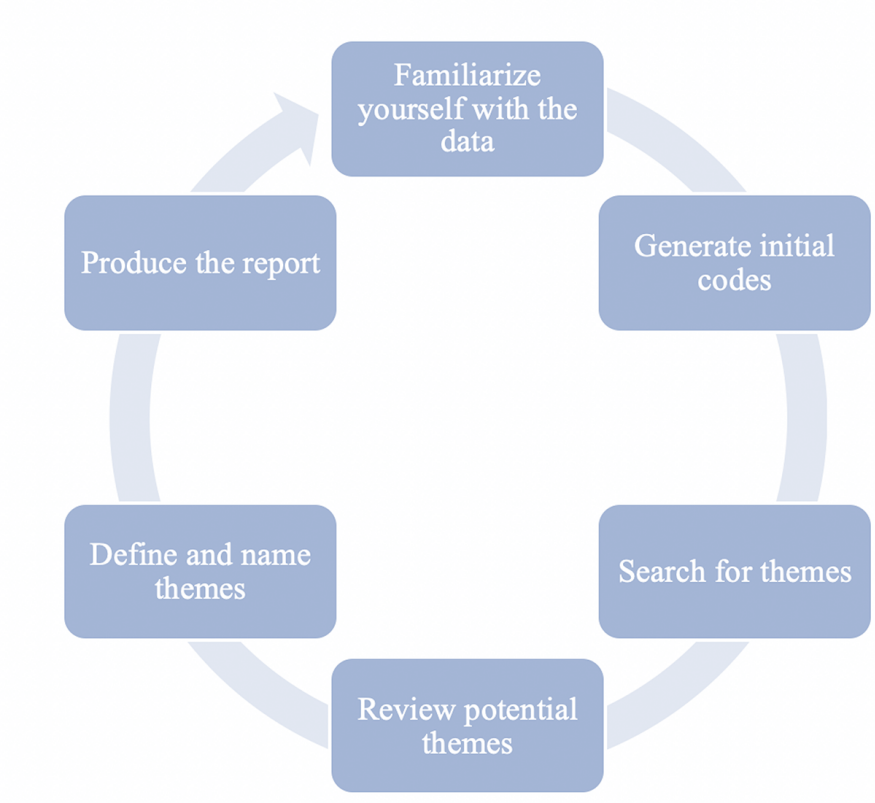

Figure 4-1: Thematic Analysis Process Source: Author-defined.

The analysis of the interview data was performed using thematic analysis of six stages introduced by Braun and Clarke (2006) as they are presented in Chapter 3 (SS 3.12). It was achieved by

familiarisation with the transcripts, the initial generation of codes, identification of patterns, the possible refinement of the themes, and defining the thematic structure on a global level. Coding and collating were done in NVivo 12 to achieve consistency and traceability of decisions.

The primary characteristic of the analysis was the combination of the inductive reasoning (that allowed creating patterns immediately out of the stories of the participants) and the deductive mapping (that was controlled by the constructs of Protection Motivation Theory (PMT)-perceived severity, perceived vulnerability, response efficacy, self-efficacy). The four broad themes determined during this repetitive process explain the manner in which Abu Dhabi SMEs were impacted and responded to the digital transformation occasioned by COVID-19.

The discussion has developed to a general overview on the effects of digital-adoption to the further study of behavioural and organisational effects of information-security management. All of the themes consist of two or more codes that signal connotative meanings of the participants rather than a detached utterance. In their capacity to build analytic transparency, representative quotes are used in all the thematic discussions to show the significant points that are also supplemented with interpretive comments on how the findings are relevant to dimensions of PMT.

The overall process is outlined in Figure 4-1 and the four themes that were retrieved are given in Table 4-2. The discussion below will be structured around the following analysis themes: (1) Impact of COVID-19 Digital Adoption on ISM, (2) Legacy of Digital Adoption on SME Operations, (3) Information Security Practises and Solutions, and (4) Resource Constraints and Capacity Challenges.

A structured codebook was developed to simplify the data categorisation and interpretation in order to ensure reliability and consistency of thematic coding process. The codebook defined key codes, inclusion and exclusion criteria and sample quotations which were refined multiple times during the initial stages of coding. This contributed to reducing the chances of subjective bias and ensured uniformity in the interpretation of textual data across the subjects. The peer review also helped in improving the reliability of the coding since a second researcher went ahead to review a subsample of transcripts and ensure that the codes assigned were correct and consistent. These differences were ironed out through consensus and addressed, and the themes polished and enhanced the analytic rigour. These procedures were done to render final thematic structure transparent and replicable, and this is consistent with the recommendations made by Braun and Clarke (2006) to guarantee credibility and reliability in qualitative research.

Table 4-2: Step 6: Report Generation

Finalised Themes	Sub-Themes	Initial Codes	Supporting Interviewees' Responses
Theme 1: Impact of COVID-19 Digital Adoption on Information Security Management (ISM)	Adjustment to remote work	Mindset shift, technological change	"COVID-19 did make a huge change. A mindset shift is not only the deployment of technology." — P01
	Challenges in remote work security	Virtual Private Network (VPN) usage, security vulnerability	"People are starting to work from home using VPN. VPN is the weakest connection to use sensitive data on it." — P03
	Utilization of cloud services	Cloud adoption, remote data access	"Since COVID-19, we have been using the cloud to access our data from anywhere." — P07
	Protecting remote operations	Data protection, high-standard security	"We have to protect employees' data during the activities, which they do at home..." — P04
	Scaling security measures	Firewall upgrade, increased capacity	"We upgraded our 40 clients to an upgraded version which is 60 e, which can afford more people at a time." — P18
	Securing remote connectivity	VPN tunnel security	"All companies now need to secure this tunnelling because all staff working from home need secure connections." — P10

Theme 2: Legacy of Digital Adoption on SME Operations	Transition to digital communication tools	Adoption of communication tools	"We started using a lot more software, like Teams and all that, because the communication was quite difficult." — P19
	Operational Efficiency through Digital Tools	Digital tools efficiency, workflow improvement	"Digital tools have streamlined our workflows, hence cutting hours spent on performing repetitive jobs down into minutes..." — P02
Theme 3: Information Security Practices and Solutions	Enhanced Security Measures	Increased security measures	"We increased our security enhancement. We have multiple products and technologies installed in our organisation to enhance security." — P02
	Implementation of strict access control	Zero trust, minimum access	"We deployed the concept of zero trust. You should only give the minimum access and minimum privileges to the data.” — P01
	Exposure to new cyber threats	Ransomware attacks, internal threats	"We had attacks from ransomware viruses; some of them were internal." — P07
	Enhancing Organisational Security Culture	Security training, employee awareness	"We run security awareness training. Every quarter we run a security awareness campaign for all of the employees." — P04

Theme 4: Resource Constraints and Capacity Challenges	Scaling and Enhancing Security Systems	Firewall upgrade, increased capacity	"We upgraded our 40 clients to an upgraded version which is 60 e, which can afford more people at a time." — P18
	Secure Remote Operations	Data protection, high-standard security	"We have to protect employees' data during the activities, which they do at home, so we have to make sure that even if the users work from home, they have the high standard of security available." — P04
	Cloud Integration and Security	Cloud storage usage, Dependence on cloud for data access	"We transfer data to cloud-based storage such as OneDrive or Google Drive for secure access from home during pandemics." — P08

4.3 Explanation of Theme Development

Theme 1 discusses how the rapid shift to digital platforms and remotely working due to COVID-19 has impacted the practices adopted in information security management by SMEs. This consolidates insights pertaining to changes within technological shifts, new tool adoptions, and shifts within security practices mandated by remote operations.

Theme 2 captures how the ways of working of SMEs have irreversibly changed: the increased digital use because of the pandemic has accelerated communication and operational efficiency.

Theme 3 discusses in detail specific practices and solutions that were initiated and implemented in order to answer the enhanced information security challenges due to the pandemic. These include advanced security measures, cultural shift toward security awareness, and tactical ways such as zero trust.

Theme 4 refers to the scaling-up challenges of security infrastructure faced by the SME or resource constraints in trying to enhance the security measures which meet the demands of a more digital and remote working environment.

4.4 Presentation and Discussion of the Main Themes

4.4.1 Theme 1: Impact of COVID-19 Digital Adoption on Information Security Management (ISM)

This theme relates to the research question 1 and 3 that address the practices and solutions adopted by SMEs in Abu Dhabi to cope with information security issues. The pandemic caused the industries to adopt digital solutions that changed the practices of ISM. As interviewees commented, due to this sudden change in working style to remote working, security threats increased in frequency and complexity. P01 observed, "*Covid-19 did make. A huge change. A mindset shift is not only the deployment of technology. COVID forced us to have employees out of our premises, working from home, and applications out of our premises*." This statement illustrates how perceived severity of cyber threats prompted SMEs to shift operations rapidly, adapting through remote-work technologies while reassessing their digital boundaries. This shift created new security challenges since the data was now outside the traditional network boundaries that every organisation had protected earlier.

These challenges are mitigated through advanced cybersecurity measures that the Company 1 integrated within its systems. P01 explained working on the very concept of Zero Trust: *"We deployed the concept of zero trust. You should only give the minimum access and minimum privileges to the data."* The focus on the Zero-Trust approach reflects SMEs' growing sense of response efficacy-confidence that strict access control can mitigate new vulnerabilities created by remote work. This focus on Zero Trust shows that nowadays, it involves a much higher level of security when dealing with remote work scenarios – hence the inability to rely solely on a traditional network perimeter as before. P02 further commented, *"We increased our security enhancement. We have multiple products and technologies installed in our organisation to enhance security."* This shows an active coping appraisal, where firms invested in multi-layered controls as an adaptive response to perceived risk.

Increased measures in the line of security during COVID-19 include advanced monitoring tools and authentication protocols, which portray how these companies are trying to mitigate evolving threats. Participants have commented that there was a need to have robust security frameworks necessary to counter the enhanced risk of data breaches within a remote work environment.

The COVID-19 pandemic accelerated the digital adoption significantly. It impinged on the practices of Information Security Management (ISM) in the small and medium enterprises in Abu Dhabi. Working at the comfort of your home posed special difficulties in terms of observance of security as well as data access. Respondents also emphasised the difficulty of remote work, especially with regard to the security

of data transmission and access. P03 noted, "*People are starting to work from home using Virtual Private Network* (*VPN), VPN is the weakest connection to use sensitive data on it."* Similarly, P04 pointed out, *"We have to protect employees 'data during the activities, which they do at home, so we have to make sure that even if the users work from home, they have the high standard of security available."* These views highlight perceived vulnerability to insecure connections, underscoring the challenge of safeguarding remote employees through VPN and secure access protocols.

When inquired about the change occurred to the way SMEs handle information security as a result of COVID-19, the participant P20 indicated, *"What have happened is that a lot of information is now digital. So, there is no hard copy information. You will not have printouts, or you will not have hand-outs or do not have business cards. Mostly everything is printed. Even if you see the visiting cards are now digital. It's just a QR code. You scan it, you get all the information. So, it's digitalized. So, I would say the digital transformation has happened more during and after Covid-19*." The shift to full digitalisation demonstrates how SMEs re-evaluated operational processes under threat pressure, reinforcing digital transformation as both necessity and strategy. These changes are augmented by the strategic shifts these SMEs have implemented to ensure achieving the required level of organisational competence to fulfil the work requirements during the pandemic.

These are some of the risks that, according to the respondents, organisations invested in several security measures to mitigate. P03 described multi-factor authentication and email security gateways put in place, while P04 showed how adoption in virtual desktop infrastructure and cloud services-maintained standards of security regardless of location. According to P05, his organisation had already done a lot toward setting up secure remote access protocols in advance. These accounts reveal response efficacy-confidence that proactive investment in authentication and remote-access solutions would effectively reduce exposure. Hence, the disruption was very minimal with a seamless transition during the pandemic.

The attack surface widened as employees were connected from different unsecured networks and devices. As P06, explained, *"Attackers and everything goes widely used. Because we were at our homes. So, everything was online."* The participant's observation shows heightened threat appraisal; as attack surfaces expanded, SMEs recognised the urgency of defence upgrades. It became imperative to adjust to newer security threats at a quicker rate than usual. Investments in advanced security solutions were necessary for organisations to overcome the increased risk of cyberattacks.

All participants identified that the COVID-19 pandemic resulted in a shift to massive cloud services. This was largely driven by the need for access to data during lockdowns and social distancing. P07 noted, *"Since COVID-19, we have been using the cloud to access our data from anywhere."* Likewise, P08

highlighted, "*We transfer data to cloud-based storage such as OneDrive or Google Drive for secure access from home during pandemics*." The adoption of cloud storage indicates coping appraisal and belief in external security measures to sustain data availability. Since COVID-19, cloud solutions were adopted seamlessly to ensure remote working that is necessary during pandemics.

Considering these threats, a need existed to improve the security at SMEs because of many digital interactions. An example is P10, which echoed the combination of Virtual Private Network (VPN) and firewall policies towards of the data sent via VPN tunnels. According to him, "*All companies now need to secure this tunnelling because all staff working from home need secure connections.*" P08 commented*, "Firewalls and VPNs were critical for ensuring secure remote access to accounting software that could not be easily moved to the cloud*." These remarks show SMEs' self-efficacy-belief in their capacity to manage remote-access risks through technical controls.

The pandemic has certainly put new cyber threats in front of organisations and revealed the weaknesses of their existing system, including text-based attacks. Participants also reported that they have already been victims of ransomware attacks and more phishing attempts. P07 reported, *"We had attacks from ransomware viruses; some of them were internal."* How Ransomware added more significance to employee awareness was reflected in the experience of P08: *"Ransomware is very dangerous; employees should know about emails containing malicious attachments*. The ransomware experiences exemplify perceived severity and the shift toward preventive awareness training to strengthen organisational resilience.

Remote work occurred practically overnight as a result of the COVID-19 pandemic and that has had its consequences regarding the information security management in these organisations. The participants gave a number of steps to ensure remote operations. Participant P11 explained the following: *"We had to update our policies allowing remote desktop connection,"* emphasizing the upgrading of firewalls and developing secure remote access for employees. P12 similarly reported that his company *"had to set up all of the employees remotely"* to allow them to secure remote access to office systems, which often required managing a step-change in process, as P12 said, *"At first you cannot monitor exactly what the employee is doing from home."* These examples depict behavioural adaptation and organisational learning, SMEs revising ISM policies to sustain secure operations.

Digital tools became integral to safe communication and collaboration in the pandemic. Both P11 and P12 described early usage of some type of proprietary/internally developed conferencing systems, and then transition to more robust systems such as Microsoft Teams and Zoom. "*We had an organisational move to Teams*," clarified P11, because of their in-house software difficulties. This was not a simple task to accomplish, however it was advantageous in making meetings within the shortest time achievable, remote working, hence efficiency in operations was boosted without compromising the

security at all. SMEs increasingly substituted in-house tools with trusted platforms, demonstrating coping appraisal through selective technology adoption.

The need to protect remote work environments encouraged companies to implement new security measures. P14 mentioned *"setting up anti-hacking software and their usage of VPNs in securing remote access"*. The additional initiatives undertaken by the company of P11 involved introduction of two-factor authentication and a switching to Microsoft 365 for to gain better security capabilities. All these measures in general indicate something more widespread, which is the way organisations expanded their security infrastructure to overcome the difficulties that arose because of remote work during the pandemic. The multiple upgrades illustrate an escalating investment driven by perceived risk, affirming how fear of loss fuels protective action. According to some interviewees, the necessity to strengthen information security was identified because of having remotely moved to work- the relocation that introduced new challenges but demanded new changes in the current security measures.

P15 clarified that the COVID-19 increased any increased security risk response to the threats that were most specifically conveyed via email. He commented, *"We try to segregate it that way. Another thing that we do to help a little bit with the control is all the managers. We always have a copy of all email, to ensure also that nobody were deleted anything in and out from our subordinate,"* he said, indicating an increase in vigilance in email monitoring and verification during the pandemic. Enhanced monitoring practices highlight perceived vulnerability and a strengthened culture of vigilance among SME managers.

Similarly, P18 narrated how the organisation had to increase the capabilities of firewalls during this period, accommodating many remote users: *"We upgraded our 40 clients to an upgraded version which is 60 e, which can afford more people at a time."* This showcases a broader trend wherein SMEs had to bolster network infrastructures to manage increased remote access securely.

P16 explained that in COVID-19, with the situation presenting firewall upgrades and Internet bandwidth increases to support remote operations, the pandemic had driven them directly in the security management practices. P19 explained how COVID-19 accelerated the pace of digital transformation because of work-from-home arrangements that affected several information security management practices in SMEs. First of all, their organisation already had some instituted ISM practices, with firewalls and its internal servers for its Enterprise Resource Planning (ERP) systems and Computer-Aided Facilities Management (CAFM) software, largely accessed via an intranet setup that provided external access by controlling it through firewalls. It meant that, during the pandemic, remote working had to be implemented, with uploading reliance on remote access tools like Any Desk and TeamViewer accompanied by a strict data access regime. *"We were forced to, for most of us, to go into remote working. We had to set up, kind of have each of them with laptops and then set up any desk or TeamViewer for*

them so that they could access their systems back in the office." These remarks show organisational self-efficacy in adapting IT infrastructures for continuity under pressure.

This shift had, therefore, demonstrated the need to increase firewall capacities and secure remote access to maintain the integrity of the internal data store. The pandemic increased the rollout and usage of the digital communication tools Microsoft Teams and Zoom, both with their security configurations that contributed to coding standards for ISM in light of this increased digital exposure. "*We started using a lot more software, like Teams and all that, because the communication was quite difficult. But then again, Microsoft Teams have their security protocol, so we did not truly have to be at that end."*

Inevitably, renewing firewall licenses or utilising communication tools is simply a part of the general trend in the fast adjustment SMEs have to remain secure while working through a pandemic. Familiarity with software minimized problems but still indicated that fast scaling of digital tools meant more robust integrated security management practices were necessary to aid in dealing with new vulnerabilities opened up by remote work environments.

The immense amount of information gathered on the role played by digital adoption in transforming operations in processes among the UAE SMEs has shown a powerful effect in enhancing the efficiency and effectiveness of operations. In numerous instances , respondents restated that phenomena occurred with the change in their digital adoptive practises led to organisational change, as it occurs in large enterprises. The introduction of digital did not only render the working processes lean, but it also introduced more than impressive and considerable changes in the performance indicators and revenues. According to the participant P07, it was possible to say that *"implementing Zero Trust security model is essential to ensure information security in an enterprise. This implies that no entity regardless of their designation or role in the department should be considered trustworthy inherently."* The implementation of Zero-Trust principles demonstrates cognitive alignment with PMT's coping appraisal-balancing access and protection.

By applying such security measures, it would require every user to carry out the authorisation and authentication procedures at the time they have to utilise organisational information resources.

Efficiency gains that come with digital adoption, participants say, are heavy in streamlining several operational workflows and automation of repetitive tasks. For instance, P02 noted, *"Digital tools have streamlined our workflows, hence cutting hours spent on performing repetitive jobs down into minutes, hence contributing to more productivity."* Another respondent P06 said the similar thing: *"Digital adoption has brought about automation, reduced human errors, and improved operational accuracy."* These accounts underline process automation as an indirect resilience mechanism, reinforcing efficiency and reduced human error.

Furthermore, the digital adoption helped in reducing errors and improved the decision-making processes. P10 responded that "*through such digital tools, they were able to detect deviations not according to their intended purpose or quicker maintenance, hence more efficiency in delivering services overall."* P10 also stated, *"We deploy digital adoption tools and resources to assess usage of software and estimate user interactions based on the collected digital data. This helps us to perform adjustments based on information, identify obstacles, and analyse usage patterns."* This reflects learning-based adaptation where real-time monitoring improved confidence in mitigation strategies.

It can result in not only efficiency not only in operations but also enhance the decision-making processes based on the from real-time and, accurate data.

The other serious impact of digital adoption as reported by the participants was the streamlining of resource allocation. The allocation of resources in the real-time in response to the dynamics of demand would be efficiently provided through digital analytics and achieve savings and efficiencies in operations. In addition, the risk and safety operations management was also greatly improved with the focus that the participants put on the degree to which they were digitally transformed. As the participants mentioned, their systems of digital monitoring-such as those with predictive analytics capabilities, which give them early warnings when there is the detection of a problem or a potential anomaly—have enhanced/improved their safety protocols to avert upcoming hazards.

Regarding the impact of digital technology adoption on information security, P01 explained, *"It did increase our costs, but from, from another angle, it did reduce an amount of risk that could have been so damaging … Today we have a successful ransomware attack every 11 seconds … 560,000 new malware. A new ransomware is being pushed every day … So the risk that our digital platforms are exposed to is enormous. And that's why the biggest value we're gaining is that we are reducing that risk, we're reducing our exposure, we're reducing our attack vector. So we're reducing the amount plus the locations and the methods that we can be compromised with through such a deployment. So those deployments that we had are definitely paying off by reducing the risk of being exposed to attacks."* The participant's reflection connects cost with risk reduction, evidencing rational appraisal of investment versus threat exposure. Participants have continuously laid much stress on these early warning systems developed via digital tools, alerting timely intervention in risks related to health and safety, thereby able to forestall operational disruptions.

The participant accounts collectively underscore the transformational compulsive nature of digital adoption on operational excellence within UAE SMEs. As such, adoption of digital technologies would thus manage to increase efficiency, productivity, and safety in operational domains for SMEs. Digital integration adoption will successfully lead to strategic shift since it embraces data-driven decision-

making and operation optimization; thus, ensuring the fact that SMEs further grow and are competitive in today's dynamic digital business environment.

4.4.2 Theme 2: Legacy of Digital Adoption on SME Operations

This theme relates to the research questions 2 and 3 that inquire about the challenges and tools concerning information security management in SMEs in Abu Dhabi. This reflects pre-existing technological maturity that positioned the SME to adapt swiftly under crisis conditions. P01 stated, *"We, as an organisation, have transformed digitally since 2014. Everything is automated. Everything is on the cloud."* The enduring effects of the digital adoption in the context of COVID-19 are the persistence of remote work and cloud-based solutions. According to the survey, the respondents stated that their organisations had been digitally progressive prior to the pandemic, therefore, the process of transitioning to it was easy. This change enabled the company to adjust fast to the pandemic needs in a way that did not cause much disturbance to business.

However, the pandemic accelerated the adoption of cloud-based security measures. As P01 explained, *"We did deploy the Secure Access Service Edge* (*SASE) concepts, which extend security to the cloud environments. Providing cloud secure access to users."* This indicates strategic evolution toward secure cloud environments, strengthening perceived response efficacy within digital ecosystems. This is where SASE and cloud brokers can be considered strategies for continuously securing distributed digital environments beyond traditional on-premises security mechanisms.

The gradual, stepwise adoption highlights incremental learning behaviour that characterises SMEs' pragmatic adaptation style. P02 spoke about the gradual enhancement of digital applications, stating, "*It's not like a major change... we enhanced also the security. But it's not like a major change; it is like step-by-step changes."* Incrementalism approach to digital adoption highlights practical changes that maintain the operations and security in a constantly evolving environment.

The pandemic-induced digitally induced adoption has had a severe impact on SME operations, which has put a permanent change towards to a more flexible, technology-based work environment. This remote working experience has seen the SMEs adopt hybrid models of working. P04 accentuated operational flexibility by observing, "*Not all engineers have to come to the office every day. They can work from home. So, our mind-set even changed."* This illustrates the behavioural flexibility that underpins sustained organisational resilience through digital transformation. This shift has enhanced productivity and allowed better utilization of office space.

The pandemic has been merely the catalyst to invest more in digital infrastructure since organisations have discovered that the latter provides extra security and flexibility in operations. P05 discussed the implementation cloud services and security solutions that came in large scales and had

become part of their operations. In terms of this method of digital transformation, it has been termed to have a positive impact. Ongoing financial commitment to security tools signals recognition of long-term digital dependency and proactive risk mitigation. As indicated by P03, "*The digital adoption during the Covid-19 has impacted our organisation in a very positive way that it made a huge difference from before Covid-19 and after Covid-19."*

There is concurrence that investment in security technologies has to be continued if organisations have to protect themselves against evolving threats. According to P04, "*We invested in some tools. This increased somehow the investment or the cost for our operation."* This means an implication of commitment over time to maintaining robust security frameworks as part of the legacy for digital adoption.

The pandemic has enforced digital adoption that has turned out to be permanent in changing the way SMEs run their operations. Cloud computing and remote work capabilities have remained central to their activity. The participant's reflection shows a shift in perceived vulnerability-from distrust in online systems to confidence in secure digital operations. P07 responded, "*Indeed, many companies now rely on cloud services and online operations: "After Covid-19, so many things converted to be online, and it's now more secure than local servers."* T*his was further supported by P10 who said, "All companies now need to go to the cloud; it is a good option for small companies."*

To explain the benefits SMEs have gained while addressing the challenges posed by COVID-19, the P21 said, "*I'm speaking from my perspective, and the other companies who I know, all of the companies who implemented the newest technologies in terms of cybersecurity, digitalisation, digital transformation, they even made much more profit. You remember post-Covid-19 before Covid-19 most of the companies were operating in the traditional way. The companies who are ready digitally, they made a lot of money, especially in the delivery sector, in the facility management, in the maintenance operations. All of those companies, they made a good profit during that time and after that time. And the main purpose of digitalisation is reducing the cost, making the business more agile, faster, reducing the cost, reducing the effort, and of course, reducing the factor of time."* .The emphasis on profitability aligns with PMT's outcome expectancy concept—linking security investment with positive business returns. This indicates that SMEs have been able to attain higher levels of performance and productivity as a result of digital adoption during and after COVID-19.

The digital turn has offered SMEs more flexibility and efficiency within operations. P08 has welcomed the cloud solutions for the portability and usability advantages they provide: "*It's more reliable, easier to use; you can continue to work from home in case of emergencies."* This demonstrates continuity planning through digital resilience, allowing SMEs to sustain productivity during disruptions. This view was corroborated by P07, who discovered that these cloud services provided access to their

data in a much more convenient and secure fashion when employees worked from home. He remarked, *"And from Covid-19 so many things convert to be online only ... by having Covid-19 like it's more secure now, the data, the way everything you have now ... Now I think it's more secure from the local server clouding ... It ensures your data will be safe as backup server, as a cloud saver. Then there are backup servers, there are more security, more fire removal, more to protect you from any attack."*

Business continuity planning has been enhanced with the adoption of digital technologies. Cloud services have provided reliable backup and disaster recovery solutions. P08 highlighted that among the value additions of cloud storage was a "*Cloud service providers give a 30-day restoring option for data recovery" f*eature, which was very vital during the disruptions of the pandemic. This has ensured that SMEs are better prepared for future crises.

Prior readiness created a cumulative advantage that enabled faster, low-risk adaptation when external pressures intensified. According to P13, the International Organization for Standardization (ISO) certification they had earlier, before the pandemic, had helped them easily shift to remote work, saying that "*digital adoption before COVID-19 laid a strong foundation."* Not only does moving to digital documentation and paperless operations bring efficiency improvements, according to P14, but it also entails cost savings: "*For me, we reduced some of the costs because we reduced, we become like paperless."* Cost reduction reinforces efficiency-driven digital transformation, a motivational factor sustaining continued technological reliance.

Those who had remote work practices established during the pandemic said the same continues to be in place. P12 pointed out that their infrastructure is now "*ready for any situation where we are called back to stay at home,"* so they will be ready when future disruptions occur. This transition exemplifies SMEs' collective learning processes and technological assimilation under stress. This feeling entirely corresponds well with P11, expressing that "*technologies of remote work, problematic at first, turned out to smoothen operations and enabled savings on operational expenses, less spent for travels for meetings."*

Many of these digital communication tools that were adopted due to the pandemic are now permanent in many SMEs. P11 showed appreciation for Microsoft Teams, which makes meeting setups easier and diminishes the necessity for physical presence. He explained the adoption of communications tools by saying, *"Basically, at the beginning, we were a bit slow to adopt the Microsoft Teams. We did develop our own software for remote, let's say, communications, but it was very problematic. So, we ended up having to move to teams as an organisation. And of course, the challenges are people getting to understand how to make teams work ... I think people slowly have adopted the video conferencing software."* It was further emphasized by P12, who added that "*It had improved the ability to track presence more easily among employees and made organizing remote work easier with digital tools."*

For example, Teams was mentioned as enabling them to easily transition to a flexible and more digital-first approach to business activities.

The adoption of digital tools, transition, and new security measures continue to influence how a business performs post-pandemic. P15 reflected on how the adoption of digital tools during COVID-19 influenced him to be more vigilant concerning security: "*Since coronavirus, I think many people have nothing to do. So, I think it's like, you know, being like hacking and all, trying to do fraud."* The observation reveals heightened risk awareness and cautious online behaviour as residual outcomes of pandemic-induced vigilance. This suggests a continuing awareness and a careful attitude towards digital interaction as a legacy from the pandemic period.

P17 pointed to the long-term benefits of strengthening these security measures: "*We got a faster network, and by upgrading the firewall, actually we got the advantage. After that, there is no hacking also."* This showcases positive reinforcement, where successful implementation reinforces confidence in digital protection measures. This has continued improving this security infrastructure with impacts that transcend just the immediate response to the pandemic, thus setting one of the positive legacies digitally transformed in enforcing COVID-19.

Furthermore, P18 stated that his organisation would have upgraded despite the pandemic, which indicates that COVID-19 had accelerated an event that would happen anyway: "*If it's not even Covid-19, it should have happened. As our company is growing, we should have to upgrade anyway."* The influential digital tools adopted, and new security measures taken in running businesses post-pandemic have been discussed by the interviewees. This suggests the lasting awareness and cautious approach toward digital interaction as part of the legacy of the pandemic period.

P17, explained to the long-term benefits of increased security, saying "*We got a faster network, and by upgrading the firewall, actually we got the advantage. After that, there is no hacking also."* This was a development in security infrastructure that emerged beyond the immediate pandemic response and hence acts as one of the positive legacies of digital transformations imposed by COVID-19.

P18 supplemented further that without the pandemic, his organisation would have, in any case, upgraded its infrastructure, thus meaning COVID-19 had accelerated an inevitable transformation: "*If it's not even Covid-19 it should have happened. As our company is growing, we should have to upgrade anyway."*

The influence of the pandemic increased its adoption of digital tools; effects were lasting on how the organisation runs its operations. The pandemic acted as a catalyst, accelerating digital maturity through necessity-driven innovation. This increase in the pace of integrating digital technologies resulted in more efficient ways of communication and improvements in operations that were planned but

accelerated due to the pandemic, as noted by P19: "*Digital adoption that was faster because of Covid-19, we thought, okay, might as well improve our systems now."*

It developed task monitoring programmes and ERP upgrades to aid in distant operations and enhance productivity. The rapid adoption of digital platforms guaranteed more efficient resource management and simplified the processes,, which marked a significant change in the operational structure towards digital solutions. P19 remarked, "*We've also implemented task tracking software in our facilities management.so you could push the job request on the phones, then they can go and complete it, and then the report will come back immediately rather than waiting for the actual physical return report."* This dependency on these digital tools that occurred during COVID-19 that ensured a shift in the manner in which tasks are handled and reported became a permanent change. This is a clear indication that digital adoption during the COVID-19 has left a permanent mark on the operations of SMEs by entrenching the use of technology into the operating fabric of the companies.

The adoption of digital technologies by SMEs has been increased significantly over the recent decades, impacting their operations and business activities extensively from the development of online products and services production processes augmented by robotic solutions, data analytics, and the Internet of Things. In this regard, P08 described the significance of digital adoption in terms of optimisation of the processes dedicated for ensuring information access and support. He asserted that *"SMEs can obtain substantial benefits from utilising digital adoption tools to offer the stakeholders, i.e. employees, partners, customers, etc., sufficient access to the related information and embracing innovation through nurturing an environment that favours creative solutions to the problems."* .This broad reflection encapsulates collective awareness that digital adoption fosters innovation, collaboration, and sustained competitiveness. This statement indicates different things regarding the impact of digital adoption on SMEs' operations. First, it is important for SMEs to provide those associated with them in any way with the information they need and this requires developing and implementing controls and systems that can protect the company's intangible assets including sensitive information. Second, adequate access to information can help the stakeholders interact with the company in a relatively more productive way, i.e., by ensuring enhanced involvement in creative activities to deliver innovation in products, processes, and business activities to build the competitive advantage. Another participant P05 explained that *"digital adoption has impacted the operations of SMEs by offering them enhanced market presence, operational efficiency, customer insights, and business agility."* This indicates that SMEs have acquired multifaceted benefits by extending their digital landscape. Digital resources and infrastructure have helped these organisations to optimise processes in different departments including marketing, finance, customer relationship, and business development.

4.4.3 Theme 3: Information Security Practices and Solutions

This theme is in alignment with the research questions 3 and 4 that address the tools, solutions, and frameworks to optimise information security in SMEs. Information security practices at company improved much in response to the pandemic. This involved monitoring and multi-factor authentication (MFA) capabilities. This indicates a shift toward a proactive security posture, where real-time monitoring builds organisational vigilance. As P01 states, "*We do use lots of monitoring tools. Continuous monitoring of our data to ensure that we reduce the chances of being exposed or compromised."* There is a more proactive approach toward ISM with principles of vigilance.

Another critical aspect was the integration of Multi-Factor Authentication (MFA) to secure digital access. P01 explained, "*We added multi-factor authentication to all of our workloads. Which means as a user, you want to log in to your email, you got to enter a code."* The implementation of MFA reflects high response efficacy, reducing perceived vulnerability during remote work. This layer of security that MFA brings is very much essential in protecting against any probable occurrence of unauthorised access in remote work.

The investment in multiple protective layers shows SMEs' growing technical confidence and belief in control over threats. P02 demonstrated similar practices: "*We have implemented many technologies that protect our data, the information inside our organization."* These technologies mean advanced firewalls, cloud-based security solutions, and endpoint protection tools - on paper, it essentially sounds very comprehensive in securing digital assets.

Finally, COVID-19 was seen to increase information security practices digitally, and new security solutions were implemented to make the organisational data safe. In that connection, participants reported more sophisticated security measures adopted to counter the increased risk of cyber threats. P03 explained further, "*Multifactor authentication, secure email gateways, endpoint protection,"* and said, "*We were implementing many email security products to their organisation."* P05 seconded, "*Proactive approach in implementing security measures with regular updates and assessment would make the system intact."* The enumeration of layered tools highlights structured coping mechanisms aligning with PMT's protection motivation process.

Employee training was identified as one of the critical facets of ISM, and the following entailed security awareness campaigns where organisations educate employees on how to identify and react to threats. P04 outlined their formal approach, "*We run security awareness training. Every quarter we run a security awareness campaign for all of the employees."* Routine awareness campaigns represent cultural institutionalisation of resilience through continuous learning. This has been effective in making the employee's eyes wide open and reducing the chance of a security breach due to human error.

Advanced technological solutions, including Virtual Desktop Infrastructure (VDI), cloud services, and secure access platforms, attributed much to the increased information security. Adopting encryption-based solutions reflects SMEs' recognition of technological safeguards as essential for credibility and trust. P06 explained further, "*We have taken up specific tools, for example, Secure Sockets Layer (SSL) certificates and secure applications that can help protect web-based interactions."*

The participants indicated the deployment of robust security measures to protect such sensitive data. P07 mentioned firewalls, VPNs, and cloud security: "*The Company has installed firewalls, and employees access the data remotely via VPN connections."* The statement underlines structural reinforcement of remote access security, balancing flexibility with protective caution. This echoes PMT's focus on coping appraisal—showing how awareness lowers perceived vulnerability. P08 added employee training to identify spamming and spoofing emails, which also surged due to remote work: *"Employee awareness is critical in dealing with spam tending and spoofing emails."*

Upgradation to security systems and frequent training of employees have become an integral part of information security management. P09 mentioned, "*We upgrade our security systems almost every two to three months." P07 reported that training on new technologies are provided to the staff as well as customers to understand the process entirely for its safe implementation."*

Participants outlined some of the essential measures in enhancing security, such as data encryption and multi-factor authentication. Policy-level adjustments illustrate procedural self-efficacy-proactive control over exposure vectors. P10 shared implementing specific firewall policies and access controls: "*We add firewall policies like blocking unused ports to prevent attacks."* Furthermore, P08 commented that remote access is more secure now, with two-factor authentication that has just been done: "*Two-factor authentication is recently implemented, making it more secure."*

Participants described the various ways that are in line to protect this information. P11 described secure server networks, firewalls, and two-factor authentication for data protection. The company of P12 put in control against data transfer from his department by hardware limitations, limited use of Universal Serial Bus (USB), and site blockages on the. These would denote a very positive slant toward securing the information since data protection seems to be considered essential and cared for by comprehensive security strategies.

Programmes for training and awareness were put forward as the key to information security. P11 trains users on phishing regularly with updates and examples of 'phishing' emails. Internal communication routines reflect collective threat appraisal and shared responsibility within digital ecosystems. According to P12, "*Companies have a culture of internal communication in which problem emails are flagged, and the employees are updated regarding security practices*." P13's organisation is

undergoing regular training that will enable the employees to remain aware of spam and phishing email threats. This puts them at high levels of ensuring a security-aware workforce.

While the majority of the respondents indicated no major security breaches, some of the probable threats put forward related to phishing and scam emails. P11 spoke about scam and phishing emails, saying that *"...there should be training given to employees to identify them and on what to do."* P12 shared an experience about a certain key logger where they realised how their organisation's alertness and multi-step verification checks aided in keeping probable data breaches at bay. This practice showcases the importance of incident response strategies in ensuring the information stays safe.

The COVID-19-induced information security practises varied in terms of upgrading of the existing systems to applying the new measures to protect against the appeared threats of remote work and the rise of digital interactions. Integration of communication and authentication tools illustrates how SMEs embedded security into daily workflows. In this regard, P16 highlighted the e-implementation of firewalls and installation of two-factor authentication in their enhanced securities: "*We have log in to Microsoft Teams if you have any meeting. And also, we have used the WhatsApp group or any other group*." The integration of these tools has helped to keep open lines of secure communication and data protection.

P18 explained that due to pandemic-related pressures, challenges in the wake of cybersecurity attacks, particularly about phishing attacks, increased: "*Some hackers have copied our same email, and they just was sending to our customer with their account details, not our account."* This incident-driven learning reinforces the value of adaptive coping and post-crisis system strengthening. Their solution incorporated security feature upgrades, adapting tighter controls for e-mail and VPN access, reflecting improvements in reactiveness toward evolving security threats.

P17 said they had adopted VPN and upgraded firewalls: "*Actually, we upgraded the firewall, the VPN, and have only used the Microsoft Team for meetings. And helped us for sharing of the work and also our ideas."* Infrastructure enhancement supports a layered defence approach-showing learned risk management over time. This adoption of existing tools in place underlines how their security practices keep improving with new operational demands.

The pro-active nature of the organisation to ISM through existing practises and solutions to digital activity as it relates to in COVID-19 is highlighted in the interview with P19. Preference for internal servers reflects risk aversion and internal control-a preventive security stance. They ensured the security with a combination of in-house servers that had restricted access to external resources, and a powerful firewall protection: "*All these data is located on our local server, in the office on site. So, it's mainly only accessible via intranet."*

Even though remote work increased, it didn't expose the organisation to sensitive data that would bodily be placed on the external networks through remote access tools logging in to internal systems and avoiding possible security risks. "*We had to increase the server license for the firewalls. We never put anything still on the web or the cloud or anything external,"* says P19.

Another component of the programmes was training and awareness where the information department would educate and sensitise the employees on the threats and dangers by making the staff abreast on spam and phishing. This is merely an illustration of the holistic nature of the ISM since it is a combination of the two factors: technical and human. P19 explained, "*We give them training when every couple of months, someone from the IT department. Will send them any latest information or news about any spam happening."* This organisation's commitment to constant security education and using already secure platforms underscores the need for integrated ISM practices tailored for evolving digital landscapes.

The participant P22 described their focus on employee training to enable their workforce to get equipped with the latest technological competencies: "*We have our HR team and also operational team. They have the workshops … So, we make sure that they should understand everything. And we have this month schedule for even weekly and monthly. Also, not only one time, but we are also scheduling every month … So, we are asking them to come, and we are giving them the training."* Ongoing human-capital investment reinforces organisational resilience through skill development and awareness. This approach shows that they consider employee awareness as an essential milestone to achieve for long-term organisational success.

The COVID-19 experience enabled SMEs to identify their weaknesses, cope with technical challenges, and understand what is required to secure information against cyberattacks. For instance, P23 exclaimed, "*All our system was hacked, specifically emails and everything, and we could not recover that data because our hosting was international hosting and we would not recover that data. It was a bit of an agony for us … we could not manage that data at that time. But it has taught us that we have to manage the data, how we can manage the data. And so now we are well and good enough. We are equipped with the certainty we have, equipped with the software and everything, how to manage the data and everything."* Experiential learning following breaches embodies resilience-building through recovery and preventive awareness.

Creation of independent secure systems reflects SMEs' commitment to sovereignty in information management. P25 emphasised ensuring high security of information to protect the interests and assets of an organisation: "*It's related to business setup and handling the clients, especially with the corporate clients. While dealing with the corporate clients, we should make sure that all the data should be very accurate and also it should be safe … we will not give anyone the access to our system. So, we have*

separated our portal, our own. For our IT team, we created their own portal and system to manage all the documents, and it was highly secure." This way they were able to avoid major losses during the crisis of COVID-19.

4.4.4 Theme 4: Resource Constraints and Capacity Challenges

This theme is associated with the research question 1 specifically that focuses on the challenges and issues of information security in the face of disruptive situations such as COVID-19. The fundamental problems that have emerged in the process of pandemic-induced digital adoption are resource constraints and capacity challenges. This quote reveals SMEs' dependence on third-party cloud providers, highlighting their limited control over critical security parameters. P01 identified the challenge of not owning all security controls within a cloud environment: "*The biggest challenge we have faced is we don't own all the controls. Amazon Web Services (AWS) or Amazon owns the controls."* Since this dependency on an external cloud provider for security controls created problems in assuring complete protection, it needed careful configuration and monitoring.

The enhancement of cybersecurity awareness and training was another critical challenge. "*We subscribed to an online cybersecurity education platform. It is now part of our mandatory on boarding process,"* P01 mentioned. Embedding cybersecurity education in onboarding illustrates an institutionalised resilience strategy through workforce awareness. It simply shows that employee training has taken centre stage to solve the human problem in cybersecurity, particularly with increased sophistication in cyberattacks during the pandemic.

P02 highlighted similar challenges related to training non-IT users: "*We found some challenges to train these users and to give them the knowledge about what we implement."* This underscores the human limitation aspect of ISM, where user awareness remains a key determinant of threat vulnerability. This statement suggests that apart from technical measures, raising awareness among users and ensuring compliance with security policies are critical in the pursuit of effective ISM practices.

Participants accepted that these security enhancements would have associated costs. "*Our investment. After Covid, multiplied by four or five times in our infrastructure,"* P01 reflected. P02 echoed this: "*It increased the cost, but. We are using it before COVID so enhancing this kind of application. Make us increase the cost, but not huge cost for our organisation."* The rapid cost escalation demonstrates SMEs' heightened risk perception and commitment to mitigating exposure despite financial strain. In any case, these measures were considered indispensable to reduce the higher risks incurred through digital transformation during the pandemic.

Sustained budgetary allocation for ISM reflects long-term adaptive behaviour, signalling evolving organisational commitment to resilience. This has meant substantial financial investment by SMEs in

new security tools and technologies. P03 commented on the implications for budgets: "*We are putting more budget every year on investing in security products."* Again, this puts pressure on financial resources as companies balance the cost of these security-minded investments against other operational needs.

The IT capabilities were scaled up by organisations to support their now-remote workforce. As pointed out by P05, "*There were maybe challenges from our team who is maintaining the system because they need to make more enhanced security, more enhanced policies."* This demonstrates internal pressure on limited IT teams, linking resource strain with operational adaptation during crisis. This emphasizes the stress that internal teams have gone through to adjust to new security demands and keep the performance of the system. Another participant, P24, asserted, "*The issue that we only had for security during that time was the work from home setup, because people had to access information through their personal Internet connection.*" Remote work was not only an effective method of doing work done during the pandemic but also presented an information security management problem.

The recurring point was the need to be constantly trained and upskilled. The participants appreciated that employees were to be constantly upscale so that new security challenges could be managed. P04 mentioned that *"Security Awareness Training had been implemented as part of Employee Key Performance Indicator (KPIs), proving an organized way toward meeting increased expectations about employee competence in ISM."* The inclusion of ISM in employee KPIs institutionalises security behaviour, ensuring continuity beyond immediate crises.

While digital adoption was advantageous, it opened multiple new avenues for cost and challenges. Participants identified the cost of implementing and maintaining sophisticated security solutions as one of them. This rationalisation highlights PMT's cost-benefit perspective-where perceived efficacy outweighs financial burden. While P08 acknowledged that the costs may be higher, he still justified it on benefits grounds: "*The cost may be a little bit higher, the benefits are more valuable."* P10 said that "*Cloud services such as AWS meant companies only had to pay for what they used, making it a good value for small businesses."*

Given that new technologies arrived and were rapidly adopted, their use required a lot of training support. P07 stated that there was a need for frequent training sessions for the staff and the customers to get used to new technologies: "*We make training for our staff and customers about the new technology and how it will secure their data."* Regular training of both employees and clients enhances collective efficacy-expanding security awareness across user layers. P08 also pointed to the shift to digital training and awareness programmes during the pandemic, which became more frequent since the security challenges increased: "*After COVID, we conduct frequent awareness sessions, maybe monthly or quarterly."*

Technical challenges for SMEs included the integration of new technologies with prior existing systems. Technical friction during digital transition underscores SMEs' pragmatic adaptation under duress. P10 explained the troubleshooting of securing VPN connections and firewall policies for remote work as follows: "*Setting up VPN access and firewall policies to work from home was quite problematic yet necessary."* P07 further introduced troubleshooting issues with cloud services and local servers, pointing out that technical support is not a one-time thing: "*There are so many; troubleshooting is constant with cloud and local servers."*

In many cases, integrating new digital technologies during the pandemic was very costly. P11 acknowledged the cost of increasing security measures and introducing platforms like Microsoft Teams, commenting: "*We had to make a budget for it*." Budget allocation underlines risk prioritization-security investments framed as indispensable rather than optional. The statement exemplifies PMT's response-cost construct, where perceived protection outweighs financial sacrifice. Similarly, P12 indicated that secure digital solutions like these are very, very costly, saying: "*When you want something secure, you pay for it.*" This underlines the tension between impactful advanced security measure rollouts at times when there is excellent turmoil around budgets.

A few of the participants brought operational issues to remote working or going digital. On this aspect, P12 and P11 responded that they had difficulties with getting acquainted and making employees continue security practises when they work t home.. P12 states that it may be difficult to know what employees are doing at home and hence verify whether what they are doing is in accordance with the security practise. The identified problems suggest that the process of information security management in a decentralised workplace is not devoid of difficulties..

The transition to digital solutions has at one point added more workload to the muster of IT and security teams. P12 meant that much more detailed support was required to be provided to remote workers regarding the establishment of secure remote access and the resolution of potential problems. Process redesign signifies SMEs' capacity-building response, aligning with resilience through adaptive learning. This is why the organisation of P14 has had to change the processes and introduce training related to digital tools and security habits of its employees. The surge in demand for IT and security resources indeed suggests that such rapid and massive digital adoption can bring extra pressures to bear upon organisational capacity. Concerning work during COVID-19, P19 stated, *"But with information security was for our people who were working remotely, that back-office staff and all, they had to access the systems here. So, we had to set up, kind of have each of them with laptops and then set up AnyDesk or TeamViewer for them to access their systems in the office."*

In support of COVID-19, SMEs were found to face prominent resource and capacity issues in enhancing the information security infrastructure. At times, among the prime challenges will be the upgrading charges for technologies and low capacity for dealing with complex security systems. Recognition of security's strategic value over its cost represents a mature, benefit-oriented risk perspective. For example, P16 acknowledged the financial load of upgrading their firewall and increasing internet bandwidth: "*…it's increasing for cost but its benefit". More than this, we are getting more benefits.*" Despite these benefits, the cost of implementing such new security measures was a significant concern to smaller organisations having limited budgets.

P17 also complained about the fact that upgrading their firewall and internet capabilities would pose budgetary challenges: "*The cost involved for firewall upgradation. That was a challenge finding for these things. It costs you too much. Yeah, more than our budget actually for that*." The reflection captures financial vulnerability in SMEs, linking constrained resources with reduced resilience capacity. This is a latent issue wherein SMEs have to balance security needs with financial constraints.

P18 also highlighted some issues about cost management associated with the remote access possibilities increase: "*Everybody can access the VPN at the same time. Otherwise, it was getting hanged like ten or 15 people one at a time when they were using the firewall get jammed. It will not work at full, then it became fast after upgradation*." The scaling of digital infrastructure showcases technical resilience under pressure and adaptive recovery. This explains or explicates how, given new demands, security measures can be scaled and increased without stretching resources to the extent.

It means the purchase of additional firewall licenses and modernization of ERP systems: it underlines the financial and logistic stress experienced when digital adoption happens fast. P19 explained, "*We had firewalls for a certain number of users … we had to increase the server license for the firewalls*." This highlights scaling limitations, where resource constraints test the elasticity of SME cybersecurity infrastructures. The general manager noticed that, although these upgrades had been necessary, COVID-19 did speed up these processes. They were generally held in plan investments that would have happened anyway, so the pandemic accelerated but did not fundamentally change their resource allocation strategy. "*It was anyway required to do these upgrades probably a year or two down the line. Covid-19 expedited the requirements*."

The fact that there was minimal price associated with using the free tools like Any Desk and TeamViewer for remote access had alleviated some financial burdens, proving it to be resourceful management in the face of constraints. Most problems encountered were logistical, related to adapting existing systems for remote work and employee communication and familiarity with new tools. Communication breakdowns highlight non-technical barriers to resilience-emphasising the socio-

organisational side of ISM. P19 asserts, "*One of the challenges was to make sure everyone was communicating... getting these communication tools widely utilized by our employees*."

4.5 Theoretical Integration of Findings with Protection Motivation Theory (PMT)

The four emerged themes show that the cybersecurity behaviour of Abu Dhabi SMEs during and following COVID-19 mostly follows the cognitive pathways of the Protection Motivation Theory (PMT), with certain deviations to the context. Overall, the results confirm that the protective measures of SMEs are based on the sustained threat appraisal (perceived severity and vulnerability) and coping appraisal (response efficacy, self-efficacy, and response cost). Thematically (Theme 1) SMEs demonstrated greater risk-awareness and risk-vulnerability in the event that their operations shifted to the online platform, which is reflective of the threat-appraisal process of PMT. The participants (P01, P03, P06, P12) indicated ransomware and phishing as a severe threat clearly, and their following implementation of Zero-Trust and multi-factor authentication models exhibit high efficacy in responding and a sense of the usefulness of protection. The rapid operational adjustment and self-belief in digital controls (P05, P11, P19) also brings about self-efficacy, which supports the claim of PMT that belief in ability encourages continuation of protection behaviour. But, the scant reference to emotional appeal to fear implies that the protecting motives of SMEs were rational as opposed to being motivated by fear an aspect that is slightly inconsistent with the conventional PMT presumption of fear as a fundamental driving force.

Theme 2 supports coping appraisal and the permanence of security habits by the continuity of digital adoption beyond the pandemic. The participants who perceived the pandemic as a catalyst of change (P01, P02, P07, P10) are the good example of how the perceived success of digital defences and the belief in internal ability maintain behavioural change-which fully aligns with PMT. Likewise, their gradual use of technologies (P02, P04) was an evaluative, adaptive process that corresponded to the dynamic logic of cost-benefit in the theory. Nevertheless, there were SMEs who defended security decisions based on benefits in productivity and profitability on the first place (P21, P14), indicating a more instrumental orientation and not a risk-avoidant one. This is a partial departure of PMT, which is conventionally held as a response to perceived threat, rather than as a facilitator of efficiency.

PMT was also proven by itself in Theme 3 by strong examples of response efficacy and self-efficacy. The extensive application of technical protection (monitoring tools, MFA, firewalls, endpoint protection (P01, P02, P03, P07, P17) and the comprehensive training of employees (P04, P08, P11, P13) proved the cognitive alignment with the assumptions of PMT about arousal of effective coping mechanisms on the basis of a perceived control and confidence in the response. Notably, participants reported the need to have budget constraints but still opted to retain upgrades and awareness programmes (P09, P25) as an

example of coping appraisal, which balances the perceived benefits and costs. In this case, PMT is well supported by empirical evidence both at individual and organisational efficacy levels, which contribute to sustained security culture.

Theme 4: SMEs faced by financial and human-resource constraints (P01, P04, P17) demonstrated that the response cost is a less-studied PMT factor that serves as a decisive (moderating) factor in protective behaviour. Even though the use of high costs at times limited adoption, adaptive coping appraisals were revealed in the use of low-cost tools and internal consolidation strategies (P03, P07, P10, P19) in accordance with the concept of rational trade-offs of feasibility and strength of protection in PMT. However, some of the findings are somewhat contrary to PMT as they reveal that even with the obvious risk awareness, some SMEs were not always able to take the necessary precautions since they lacked the resources-which is a reasonable limitation in a more practical context that the individual-focused model of PMT fails to reflect.

On the whole, this research proves the relevance of PMT in describing the process of SME cybersecurity decision-making and unveils its contextual constraints in a setting with limited resources. The similarity is found in the cognitive chain of risk perception to protective action and the dissimilarity is evident in the fact that financial, infrastructural or institutional facts take precedence over theoretical anticipations of rational, threat-driven behaviour. Thus, the combined results further develop PMT by establishing adaptive resilience, which is based on organisational learning, cost awareness, and incremental coping, as the situational manifestation of protection motivation among the Abu Dhabi SMEs.

CHAPTER 5: DISCUSSION OF FINDINGS

5.1 Core Aim of the Study and Theoretical Focus

This paper has covered the impact of COVID-19 on the use of digital adoption in informing the management practises of information security management practices among Small and Medium Enterprises in Abu Dhabi. This rapid transition to digital platforms and working from home raised the levels of cyber threats, consequently exposing SMEs directly to many forms of vulnerabilities regarding information security. Through an evaluation of the various protective strategies and solutions adopted by these companies to mitigate threats, the results reflect how SMEs can be strengthened in this regard in taking on the rapid digitalisation of today's world.

The Protection Motivation Theory. has largely been the centre of concern in the formulation of the theoretical foundation of this research. According to this theory, individuals and organisations will embrace protection behaviour during an occurrence of what is perceived to be high levels of threats, and at the same time will be in a position respond effectively. The PMT was applied in this way therefore, offered a prism of background through which the perceived threats impacted SMEs in their adoption of cybersecurity practises. As per PMT, the findings indicate that the level of threat that SMEs had about cyber threats during and after theCOVID-19 directly related to protective behaviours that SMEs had. That is, as more people go online, the perceived risk has also increased and the have responded accordingly by taking real action to improve cybersecurity despite their financial and logistical limitations.

5.2 Findings of the Study

The results of this study have emphasised that cybersecurity threat can be considered as fundamentally important to consider in implementing digital technology. Thus, the evaluation and control of cybersecurity threats are critical operations within the framework of information security management implemented by SMEs in Abu Dhabi, namely, in the conditions of COVID-19 pandemic and after it. Similarly, the underpinning by the fraud triangulation theory can be aligned with this study’s findings. This theory underpins three elements that lead to the occurrence of fraudulent activities: motivation, opportunity, and rationalisation to commit fraud. This also relates to the human psychology and behaviour when individuals confront a certain situation in terms of benefits and gains. The current study also endorses the fact that fraudulent activities are more likely to occur in scenarios where sufficient measures and systems are missing to prevent cyberattacks.

The major challenge faced by SMEs operating in Abu Dhabi related to information security management as a result of COVID-19 related digital adoption is the dependence on the external cloud

providers for security controls. Many organisations cannot ensure complete cybersecurity because they do not have direct control of the critical elements involved. This is a significant weakness that exists in the cloud-based environment, where effective control of security does not depend on their own configurations and practices. For this reason, organisations need to carry out necessary monitoring as well as management practices to lessen the threats probable to arise in this scenario, which necessitates increased awareness and better control over security in case of third-party providers.

Relatively most of the major barriers to expanding information security relate to financial constraints. The COVID-19 pandemic caused huge needs for investment in new security technologies such as advanced firewalls and cloud services. Such an increasing cost turns out to be a heavy load on the budget of a small or medium enterprise and often compels many of them to spend a considerable share of their financial resources in maintaining and upgrading the security infrastructure. While such investments are justified by the need to protect against growing cyber threats, they also challenge organisations that have more limited financial flexibility and, therefore, affect their overall operational capacity.

Remote work management is one of the most critical challenges in Abu Dhabi SMEs. As the SME needed to upscale their IT resources to handle the increasingly dispersed workforce by providing secured private connections and managing firewall policies among other tasks at a rapid pace. This shift did not only result in increased workload to IT teams, but also logistic and technical difficulties. Contributing to the problems encountered by the SMEs is the ongoing training and upskilling requirements, as they have to do extra efforts to ensure the employees are updated about new technologies and security procedures. This ever-present need of training causes capacity strain as these SMEs must balance effective security with realities in dealing with a remote workforce.

The issues of integration have characterised the operationalisation of new digital technologies with the systems in place. The issues with the remote access and security adjustment that are required to access to the new digital platforms have been experienced in SMEs. Their solutions have taken long durations of troubleshooting, including support, which put further strain on the organisational resources. In fact, the necessity of regular updates and maintenance of security systems speaks to the challenges that exist, and it can be seen how digital adoption can be followed very fast and with its advantages as well as serious logistical challenges.

5.3 Aligning Research Questions with Findings

The connection between the research questions and the study findings is important to explore in order to draw conclusions regarding the main issues addressed in the study. The major research questions that were considered in this research were:

1. **How has the digital adoption driven by COVID-19 impacted information security management practices in SMEs in Abu Dhabi?**
2. **What strategies, tools, and frameworks can effectively address the cybersecurity challenges faced by SMEs in Abu Dhabi during the COVID-19 digital landscape?**

In this section, it is shown how the research study effectively addresses these research questions, by presenting an integration of the findings, theoretical frameworks, and practical applications.

5.3.1 Impact of COVID-19-Driven Digital Adoption on Information Security Management Practices in SMEs in Abu Dhabi

The first research question is concerned with assessing the impact of covid-19-driven digital adoption on information security management practices in SMEs in Abu Dhabi. The findings show that the digital adoption brought a new paradigm shift to the cybersecurity risks in the SMEs in Abu Dhabi. As organisations migrated to the cloud, include as work from home and other online business models, the importance of ISM practices was realised. The study shows that because of resource constraints and lack of expertise, SMEs failed to put in place a robust security control and therefore vulnerable to cyber threats.

5.3.1.1 Increased Cybersecurity Threats and Perceived Risks

One of the main outcomes of accelerated digital transformation was the growth of the perception of cybersecurity threats. They experienced a higher probability of phishing scams, ransomware, or unauthorised access since they had extended their digital networks. This is in line with the Protection Motivation Theory (PMT) that states that high perception of threat leads to protection motivation. Small and medium enterprises enhanced general security protocols in light of the new cybersecurity measures such as firewalls, multi-factor authentication, and endpoints.

5.3.1.2 Shift Towards Cloud-Based Security Models

The study reveals that there has been a growing trend of cloud-based security platforms with most of the SMEs depending on cross-cloud security measures that include cloud service providers for their cloud data storage, cloud collaboration tools and cloud security solutions. Although the implementation of cloud services brought operational agility, it exposed new risks since SMEs did not have much control over the cloud security settings. The reliance on external cloud providers made it mandatory for business to embrace new risk management paradigms like audit and compliance to prevent security threats.

5.3.1.3 Financial Constraints and Resource Allocation Challenges

The shortage of funds was among the notable challenges that SMEs faced in their operations and this influenced their endeavours in implementing advanced cybersecurity practises. Some of the

expenses that led to the barriers were the cost of acquiring and deploying advanced security controls that also encompassed intrusion detection systems and zero trust security models. Consequently, many SMEs had to focus on low-cost strategies like training and creating awareness among the employees to improve their cybersecurity. As pointed out in the study, despite the fact that SMEs understood the necessity of cybersecurity expenditures, budgetary constraints meant that they were mostly only able to implement security measures reactively.

5.3.1.4 Challenges in Remote Work Security

Remote work can be said to have been a double-edged sword for SMEs. Although it helped organisations to continue operations during the COVID-19 pandemic, it brought new risks including compromised home networks, use of personal devices, and social engineering threats. SMEs were forced to quickly adopt VPN, endpoint security, and access controls to protect newly adopted remote working models. This work revealed that most of the SMEs faced challenges in the implementation of security policies for remote work environment mainly because of the ignorance of the employees and the absence of mechanisms to monitor their compliance.

5.3.1.5 Regulatory Compliance and Information Security Governance

Due to the change in the nature of threats, SMEs had to ensure that their ISM practices met regulatory compliance and standards. The study shows that there was a growing concern for compliance with UAE's cybersecurity regulations, data protection laws and other related guidelines among the SMEs in Abu Dhabi. Nevertheless, compliance enforcement was still an issue mainly because there were few dedicated cybersecurity employees in SMEs. In many cases, organisations depended on outside consultants or outsourcing to guarantee compliance with the rules.

5.3.1.6 Adoption of Proactive Security Strategies

The study also shows that there is a growing trend of preventive security measures by SMEs. Those companies that suffered cyberattacks in the initial years of businesses' digitalisation paid more attention to preventive measures, risk assessments, security and incident response planning, and training. This is in line with the PMT framework since SMEs realised the need to take preventive measures in the future. New Security models such as the "Zero Trust" where access to users is granted based on the principle-of-need also became apparent among the SMEs as a method of improving the security measures.

5.3.2 Strategies, Tools, and Frameworks to Address Cybersecurity Challenges in SMEs During the COVID-19 Digital Landscape

The second research question deals with finding out the best strategies that can be employed to address cybersecurity issues in SMEs. The analysis shows that the subject SMEs in Abu Dhabi used both IT solutions, organisational measures and cybersecurity standards to improve the security position.

5.3.2.1 Implementation of Cybersecurity Tools

It shows that the majority of the SMEs apply various categories of cybersecurity solutions to reduce risks and enhance their security conditions. The most commonly embraced one was the firewall and endpoint security solutions that helped SMEs to secure their network infrastructure against unauthorised access. The assistance of the newest technologies in firewall enabled the companies to establish a wall between the external threats, and the endpoint security served to secure the devices that connected to the business network against malware and cyberattacks.

Multi-Factor Authentication (MFA) was another strategy that was identified to be employed by SMEs as it was identified to be a cost-effective but efficient manner of handling the issue of unauthorised logins and credential-based attacks. MFA is a security tool, which involves the use of one or more variables to confirm the identity of the user, thus reducing the possibilities of unauthorised parties gaining access to the systems. Moreover, many SMEs had adopted Data Loss Prevention (DLP) systems to control and guard leakage of valuable business information. Such systems provided a real-time track of the information being shared hence minimising the possibilities of leakage of sensitive information whether by accident or sabotage.

Other SMEs also installed Intrusion Detection and Prevention Systems (IDPS) which in turn would assist them in detecting and deterring cyber threats as they happen. These systems kept the network activity under check and intervened in case of any security threats that were likely to occur. Through the implementation of the above cybersecurity tools, SMEs were able to enhance their protection, minimize risks, and establish a more secure IT environment due to the growing threat posed by the COVID-19 and its consequent promotion of digital transformation.

5.3.2.2 Employee Training and Security Awareness Programs

The most effective interventions that were found in the study were the establishment of cybersecurity awareness programmes for the employees. Since people are still a significant source of security breaches, SMEs implemented awareness programmes to teach employees about phishing, password, and data security. From the study the conclusion made is that SMEs that practice security training were reluctant to security threats and complied with internal security policies almost all the time.

5.3.2.3 Zero-Trust Security Framework

The results of the study reveal the increasing interest in the Zero-Trust security model for SMEs. This model is based on the model of “never trust, always verify” where all users and devices are authenticated before they are allowed to access sensitive resources. This was achieved by the adoption of the role-based access controls and constant monitoring of the systems by SMEs to minimize insider threats and credential theft.

5.3.2.4 Managed Security Services and Third-Party Cybersecurity Support

Because of this, most SMEs had to outsource their security services from other cybersecurity organisations due to resource constraints. The studies show that outsourcing security management was beneficial for SMEs as they could rely on experienced threat monitoring, incident response, and compliance management without employing their own cybersecurity staff. Although, outsourcing improved security efficiency, it also brought new issues of data privacy and reliance on third parties.

5.3.2.5 Regulatory and Compliance Frameworks

In order to manage cybersecurity threats, SMEs began to integrate their ISM practices with the existing cybersecurity frameworks and regulatory requirements. Organisations in the study indicated that numerous SMEs incorporated the ISO/IEC 27001 or international standard for ISMS on information security to develop a systematically managed security system and manage risks. This framework helped the businesses to develop systematic process of identifying, controlling and managing the risks in order to improve its cybersecurity status. Moreover, the UAE SMEs complied with the National Electronic Security Authority (NESA) Guidelines that offered certain rules and regulations for the UAE business environment. These guidelines assisted SMEs to enhance the security measures in place, meet the national cybersecurity requirements and safeguard business data from cyber risks.

Another important area for SMEs with international activities was the General Data Protection Regulation (GDPR) compliance. Companies dealing with personal information of European Union citizens incorporated GDPR-compliant data protection features to improve the clarity of the data, protect the consumer data, and avoid the consequences of violating the GDPR regulation. As such, by following these frameworks, SMEs succeeded in enhancing their capacity to mitigate cybersecurity threats while at the same time, they embraced compliance, privacy, and information security principles within the emerging digital business environment.

5.3.2.6 Incident Response and Business Continuity Planning

The other notable finding that was arrived at in the research was the importance of incident response planning in the management of cyber risks. The research also concluded that firms that had been targeted by cybercriminals were likely to have appropriate plans to of responding to the attacks to prevent a significant amount of time and data being lost. Business Continuity Planning (BCP) was also carried out as SMEs adopted backup strategies, disaster recovery, and redundancy to maintain business continuity.

The research results give clear and exhaustive answers to the research questions which show that COVID-19 forced digitalisation had a significant effect on information security management in SMEs. As a result of digital transformation, change in operational measures affected the ways in which SMEs

addressed cybersecurity issues, such as through the implementation of strategies, tools and frameworks. Lack of financial resources, absence of specialized personnel, and compliance issues are still contemporary challenges that affect SMEs; however, better security measures like Zero-Trust frameworks, employee education, and cloud security advancements have been implemented to improve the security of SMEs.

Thus, by applying PMT and the fraud triangle, this study enriches the knowledge of the cybersecurity situation in SMEs in Abu Dhabi in the context of a post-pandemic world. Future studies could be made to assess the long-term viability of these cybersecurity measures as well as the success of their use in preventing new threats in the growing environment that reflects the business world heavily entrenched in technology.

5.4 Key Findings and Achievement of Research Objectives

5.4.1 Objective 1: Evaluate Information Security Practices in SMEs following COVID-19-related Digital Adoption

The study addresses this objective by identifying the prevalent information security practices adopted by SMEs in Abu Dhabi to mitigate the risks of cybersecurity in relation to digital transition. A notable practice was moving to cloud technology, where operational continuity, through working from home, was assured, complemented by increased data accessibility. This transition brought in new security challenges, i.e. an increasing dependence on third-party providers and a limited control that SMEs have over these third-party services. SMEs tried to secure the remote operation by using firewalls and endpoint security solutions. These are parallel actions to PMT, as SMEs realised increased vulnerability and changed their security practices and routines accordingly. The "Zero Trust" frameworks have also been implemented by SMEs to restrict user access to only the resources that are deemed essential for business operations, adopting the practice of information security in multiple layers. This shift showed that an increasing number of SMEs was becoming aware of the need for reducing rights and permissions (an action corresponding with PMT), calling for proactive and preventive defence against a threat that may arise any time.

5.4.2 Objective 2: Conceptualise Information Security Challenges in SMEs during the COVID-19 Pandemic

This research considered in detail the cybersecurity challenges faced by SMEs during the pandemic. The main insights gained were that fast digital tools adoption put SMEs at a risk of less threatening threats in the past such as phishing and ransomware attacks, overreliance on remote access solutions

such as VPNs, and bandwidth constraints of cybersecurity infrastructure. Integration with legacy systems has also put SMEs at risk of disrupting and jeopardizing further security and operations.

Telecommuting also caused certain tension in resources: there was a sudden necessity to train IT departments to work with dispersed employees. In this regard, this resource tension illustrates the opportunity perspective of the theory of the fraud triangle theory which opined that cybercriminals seek organisational vulnerabilities where organisations are facing stress or uncertainty. The relevance of PMT in SME cases is also justified by the fact that most of the businesses have been adopting improved security measures as a measure to enhance their security against perceived threats at the expense of financial pressure.

5.4.3 Objective 3: Identify Tools and Solutions Addressing Information Security Challenges Related to COVID-19 Digital Practices

The study addresses this goal by discussing particular cybersecurity tools and solutions used by SMEs including firewalls, endpoint security, and cloud-based storage solutions. The use of clouds has been significant to SMEs in terms of how to deal with the data access and collaboration requirements in the remote settings. The exercises of firewalls in protecting the networks, combined with high end point protection were realised to minimise the vulnerability such to such cyber threats by a very large margin.

The other important research outcomes of the study are employee training, which means that organisations must possess a suitable security culture. This is also in line with the focus of PMT which is taking the steps to guard against perceived threats. Although the use of Zero Trust indicates that SMEs are dedicated to managing risks internally, it is rather compatible with the aspects of PMT because access is limited in accordance with the job requirement, thus limiting the security risks internally.

5.4.4 Objective 4: Develop a Model for Best Practice in Information Security for SMEs

The results of the research were the foundation of the best-practices model of ISM among SMEs that emphasises on layered defence strategy, regular employee training and dependence on sophisticated security technologies. The SMEs will invest in scalable, cloud-based systems that have increased their security measures to suit the remote working environment. This model conforms to the PMT since it influences an organisation to assume systematic precautionary steps. Another major point of this model is the emphasis on promoting a powerful model of training employees to adhere to cybersecurity and ensure they are aware of imminent threats.

To sum up, this research study has achieved its objectives relating to the exploration of security practices, challenges, and solutions adopted by SMEs in response to COVID-19-related digital transformation. This research not only contributes to a better understanding of cybersecurity needs but also practically supports the resilience of SMEs against future disruptions.

5.5 Linking Thematic Findings to Literature

In the following discussion, the alignment of the current research findings with those put forth by previous studies has been elaborated, considering specifically the extent to which research questions have been answered.

5.5.1 Information security practices in SMEs adopted in the wake of the COVID-19 pandemic in Abu Dhabi

The first research question (RQ) of this study is centered on what is mentioned in the above heading. Relating to this RQ, the research findings have been presented in the following sub-sections, along with a comparison of these findings with the supportive or contradictory evidence from the existing literature.

5.5.1.1 Adopting Cloud Technology

Findings of this study indicated that the COVID-19 pandemic has had a profound impact on the way businesses operate, and SMEs have been no exception as per the analysis. Employees including the Project Manager and the IT Manager argued that their companies have turned to cloud technology as a means of adapting to the new normal. It is because of its flexibility and scalability, added to its cost-effectiveness that cloud technology becomes increasingly important for the survival of SMEs in these times when uncertainty remains a significant issue for businesses. From remote work and collaboration to data management, anything that an organisation may require, cloud technology has become an integral part of the SME landscape based on this analysis. These findings correspond with the results of the previous related literary studies such as those carried out by Younies and Na (2020); Alketbi, Nasir and Talib (2018); and Rea-Guaman, Calvo-Manzano and San Feliu (2018), stating that in the next years, cloud technology adoption will rise among SMEs due to the after-effects of the pandemic and the emergence of an increasingly digital world. Qualitative analysis carried out by Ahmed and Nanath (2021) led them to conclude that SMEs enjoy many the advantages cloud technology can avail.

Results of current research highlight that the cloud technology provides the option to work from anywhere and at any time; highly relevant during the pandemic, which Cusmano and Raes (2020) have also advocated how businesses have had to shift to remote working to protect their employees and customers. Hence, SMEs can enable their employees to access data applications from anywhere, using any device, with the help of cloud technology, which will facilitate business continuity even in unforeseen events like the pandemic, as identified by Sena and Bhaumik (2021). From the thematic analysis, it was also identified that cloud technology enables smooth collaboration among employees even when working from different locations. In addition to this, Mutu, Vassilev, and Tabany (2021) explain that cloud-based applications hugely facilitate the employees in sharing files to share for access, communicate with others, and work on projects in real-time without taking into consideration their

geographical dispersion. This becomes particularly essential to SMEs, which, because of the scarcity of their resources, need to ensure that their employees collaborate well and effectively even when they are not co-located, explain (Lanz and Sussman, 2020).

5.5.1.2 Security of Data and Systems

Apart from the implementation of the use of cloud technology, this study shows that SMEs have to ensure that their initiatives for the security of their data and systems are effective and sufficient. Younies and Al-Tawil (2020) further discuss that implementing firewalls and security measures at the endpoint constitute a crucial part of a comprehensive cybersecurity strategy. Firewalls create a barrier between the internal network and the public internet, helping to prevent unauthorised access and malware. Pipikaite and Davis (2020) also discuss that firewalls help in preventing hacking, phishing, and other malware attacks. According to the employees, SMEs can implement firewalls that block malicious traffic and limit access to the authorized people and systems. This study establishes that fraudulent activities against SMEs are likely to occur in situations where adequate measures and systems are absent to prevent cyberattacks. Security measures have been discussed in the extant literature to be essentially adopted by businesses in order to prevent cyberattacks. For example, Jayarao, Ray and Panigrahi (2024) informed about measures of endpoint security, which is one that provides protection for the network based on the single devices like laptops, mobiles, and servers. Employees need to be provided with different tools and practices for end-point security which includes the implementation of antivirus software, encryption, and device management policies. Alketbi, Nasir and Talib (2018) describe endpoint security measures help to ensure that sensitive data remains secure, even if a device is lost or stolen, and that employees are only able to access the systems and data that they need to perform their job. Together, firewalls and endpoint security measures provide a multi-layered approach to security that helps SMEs protect against cyber threats.

5.5.1.3 Specific ISM Practices adopted by SMEs

According to thematic analysis, it has been identified that dependency on external cloud service providers has created cybersecurity threats for the companies. This aspect has been supported in the research by Adeusi et al. (2024) who raise a significant concern that while cloud technology provides many benefits, it also introduces new security risks, which must be addressed through the implementation of appropriate security measures. In addition to this, based on the thematic analysis, it is clear that physical control practices have been adopted as well in SMEs. For example, physical access to a building, server room or other sensitive areas is restricted to authorised personnel only. Correspondingly, Cusmano and Raes (2020) and Lee (2020) indicate that restricted access to data can be ensured through the use of key cards, biometric authentication systems, or security guards. Based on this study's findings, it is evident that SMEs, e.g. those in the IT industry, who have adopted cloud

technology also invest in protecting data centers. Data centers are critical infrastructure and should be secured with appropriate physical security measures, as mentioned by Younies and Na (2020). This may include security cameras, access control systems, and fire suppression systems. Along with data centers, such SMEs have adopted asset management.

5.5.2 Common information security challenges in SMEs in the wake of the COVID-19 pandemic in Abu Dhabi

As per the first RQ of this study as indicated above and linked to the findings of the study, small and medium-sized enterprises (SMEs) frequently face a variety of obstacles when attempting to implement cybersecurity measures, and one of these obstacles is a lack of awareness. After conducting the analysis, the conclusion can be drawn that a lack of awareness regarding cybersecurity among the owners and employees of SMEs is a significant challenge. For instance, the middle manager in IT asserted, *"Employee awareness is critical in dealing with spam tending and spoofing emails."* Similarly, a senior manager in operations highlighted that *"Apart from technical measures, raising awareness among users and ensuring compliance with security policies are critical in the pursuit of effective ISM practices."* This is especially true now that COVID-19 has led to digital adoption in Abu Dhabi.

Indeed, both Chidukwani, Zander and Koutsakis (2022), and Grassegger and Nedbal (2021) endorse that SMEs are much more vulnerable to cyberattacks nowadays, given the ever-greater utilization of remote work and online transactions, as well as cloud-based solutions in general. Younies and Al-Tawil (2020) identify that many SMEs lack either the resources or the expertise necessary for putting in place effective cybersecurity measures; another possibility even exists that these businesses are unaware of the potential risks associated with the use of digital technologies. These types of unawareness lead to security breaches like phishing scams, ransomware attacks, and stolen data, as Rosencrane (2022) found out. Besides this, Mishrif and Khan (2023) highlight that it is utterly an important thing for any SMEs to understand the importance of cybersecurity and take measures in that direction to protect themselves and their customers. It can include firewalls, installation of antivirus software, two-factor authentication methods to verify the identity of an individual trying to access certain information, and even training and educating the employees on how best to take care of data security.

In this respect, the thematic analysis in the current study indicates that SMEs mostly possess insecure technological resources. Small and medium-sized businesses may lack the financial ability compared to large corporations to invest in good cybersecurity measures or employ IT professionals as full-time workers to manage their technology infrastructure. Following that, Bakdash et al. (2018) elaborated that SMEs may be still dependent on versions of software and hardware that potentially are not supportive of the latest upgrades of security or have specific vulnerabilities that are easily exploitable by a cybercrime criminal. In relation to this context, findings suggest that cybercrime criminals will face

fewer difficulties in theft sensitive data along with unauthorised access to cloud systems offered within IT industry-based SMEs.

This agrees with Miloslavskya and Tolstoy (2019) who noted that SMEs typically do not have the technological expertise that is required to duly identify and mitigate cybersecurity risks, which can result in a lack of understanding about possible impact of cyberattacks and thus leaving SMEs unprepared to deal with security breaches. Jayarao, Ray and Panigrahi (2024), on the other hand, argue that in this respect, a weakness of inadequate information security policy remains one of the key causes which hinders the effectiveness of SMEs or Small and Medium Enterprises. This also applies with regard to the rise in digital use due to the latest technological development and the COVID-19 pandemic. Ahmed and Nanath (2021) have cited that SMEs lack proper guidelines and procedures on how data and information systems can be protected against any form of potential cyber threats since an effective information security policy has not been adopted. Therefore, from the comparison of the inferences from this study's data analysis with previous literary studies, it can be established that the major factor which contributes to their inability for the SMEs to turn up with appropriate security implementations has been their lack of an information security framework. The thematic analysis also points out in this study how vulnerable SMEs are to social engineering attacks. For instance, one respondent gave the following comment: *"We realize that our SME is not fully capable of training our staff against cybersecurity threats, especially social engineering. Most of us are really not aware how these attacks have grown in sophistication."* Such findings substantiate those from Thekkoote (2024), on the vulnerability of SMEs among other types of organisations where social engineering attacks occur.

This has also been explained by Zawya (2022), because SMEs do not have the resources to invest in sophisticated security technologies or train their employees to recognize and act when social engineering scams occur. Consequently, most of the workers may become less aware of the threats from social engineering. Hence, they may easily fall into this kind of attack. Grassegger and Nedbal (2021) also importantly discuss that trust and familiarity among workers in SMEs may be used by social engineering attacks. In such situations, it will become easier for the attackers to trick the employees into accessing any sensitive information. An example could be when a cybercriminal sends an email posing as a colleague or even a business partner, asking questions that contain sensitive information or requesting the recipient to click on a link directing them to a malicious website (Zarrouk et al., 2020). Another respondent elaborated, *"The pandemic has forced several people to work from home, thus raising the vulnerabilities to social engineering attacks. Many of our employees in the company work with personal devices; often, those do not have advanced security measures that we would really enforce on office systems. We have noticed attempts where cybercriminals posed themselves as IT support and sent phishing links supposedly for VPN updates."* Similarly, Venkatesha, Reddy and Chandavarkar

(2021) argued that the COVID-19 pandemic has increased the use of remote work and online communication, making it simpler for cybercriminals to impersonate legitimate employees or businesses and launch social engineering attacks. This has led to an increase in the number of social engineering incidents (Shepherd, 2022). The use of personal devices and home networks for work can also increase the risk of these attacks. This is because personal devices and home networks may not have the same level of security as the devices and networks provided by the company.

5.5.3 Tools and solutions addressing the information security challenges while adopting COVID-19 related digital practices

Regarding the second RQ of the current research, as depicted in the above heading, the findings indicate that significant information security management tools identified for SMEs are Distributed Denial of Service (DDoS) protection services and Data Loss Prevention (DLP) systems. The use of these tools has also been endorsed by previous researchers. In fact, according to Pillai and Polimetla (2024), both DDoS protection services and DLP systems are essential, as both are two key elements of cybersecurity management which may help SMEs protect their critical data and systems. Pipikaite and Davis (2020) stated that DDoS protection services are designed, differently, to defend against the DDoS attack-a form of cyberattack intended for making machines or networks unavailable by flooded network or server with traffic that is above its capacity. On the contrary, DLP systems prevent unauthorised disclosure, which includes sensitive data, intellectual property, financial information, and personal details. DLP systems can detect and block attempts of data exfiltration, whether intentional or unintentional, and provide SMEs with the capability to show full visibility and control over their data. According to the explanation by Pawar and Palivela (2022), the installation of high-end firewalls is one appropriate manner in which SMEs protect critical data and systems from cyberattacks.

Firewalls are network security appliances responsible for observing and filtering both incoming and outgoing traffic on the basis of predetermined rules (Lanz and Sussman, 2020). Advanced high-end firewall appliances provide intrusion prevention, application control, and deep packet inspection, among many other features, to SMEs, further building capacity in protecting against cyber-attacks. In particular, high-end firewalls can help SMEs prevent malware infections, phishing, and brute-force attacks through cyberattacks by locating and blocking malicious traffic (Younies and Al-Tawil, 2020). They could also facilitate SMEs to gain higher visibility and control of the network traffic, which in turn can enable them to monitor and manage network activity in order to spot all sorts of potential threats. Besides the technical solution, some administrative practices identified through analysis concern the making of a cybersecurity policy spelling out the expectations of the organisation for cybersecurity practices and compliance.

The policy should cover key areas which include data protection, access controls, incident response, and employee training. As suggested by Chen and Hai (2024), risk assessment is another good practice

that organisations should observe in the fight against cyber threats. In addition, SMEs have to regularly calculate the cybersecurity risks for which they are found vulnerable to take remedial action (Tully and Mohanraj, 2017). This assessment should include an evaluation of the organisation's technology, data assets, and business processes. In addition to this, it is concluded that it is important to conduct employee training, implement access control, and perform background checks.

5.5.4 Addressing SME cyber challenges with the development of an associated model for best practices

In relation to the second RQ of the study, as evident from the above depiction, the findings highlight certain important factors, as discussed in the following, which are essential to be considered when reflecting on the research findings. On the one hand, social engineering, business culture, cyber defence, and outcomes impact cyber vulnerability of SMEs. On the other hand, it is crucial to take into account cyber threats, challenges, and national regulations to determine the extent to which SMEs are in need for implementing best practices.

The findings of thematic analysis indicate that social engineering attacks have high possibility to affect the assets and security of SMEs as these companies demonstrate a considerable lack in sufficient human, technological, and financial resources to combat threats to their information systems, especially amidst times of crisis and disaster such as COVID-19 when business processes and transactions are mostly carried out online due to disruptions in general mobility and employees are not trained in sufficient number to handle cyber threats. Comparative to these analysis findings, Hijji and Alam (2021) and Lallie et al. (2021) assert that SMEs usually do not have clear guidelines and procedures and effective information security policies in place to protect their data and information systems from potential cyber threats. Minnaar (2020) and Marhad, Abd Goni and Sani (2024) endorse the current study’s findings that among the important measures are restricting unauthorised access to sensitive information and identifying and blocking malicious traffic through implementation of high-end firewalls to prevent cyberattacks, i.e. malware infections, phishing, and brute-force attacks.

An inevitable aspect of SMEs’ information security management indicated by the current research is related to the culture and values that guide decision-making, interpersonal workplace relationships, and individual performances. This is further endorsed by Ivaldi, Scaratti and Fregnan (2022) and Rafli et al. (2024) who argue that organisational culture makes it favourable for adopting new technology and preparing employees for acquiring new skills. A culture reluctant to embrace digital information systems for enhancement of operational efficiency and implementing corresponding measures will lead to increased organisational vulnerability in the face of possible cyber threats.

Moreover, this study establishes that certain factors including uninterrupted organisational operations, reduced financial losses, and enhanced employee trust play a critical role in optimising business outcomes through minimal losses to tangible and intangible assets. It is also notable that the UAE regulations to direct information and cybersecurity management issues must be comprehensive, focused, and result-oriented to combat challenges faced by the industry (Alhajeri, 2022). The ultimate finding of this study highlights the need for developing a holistic approach to deal with the internal and external environmental challenges to reduce SMEs' cyber vulnerability by adopting best practices in eliminating cyber threats and reducing the number of information security risks.

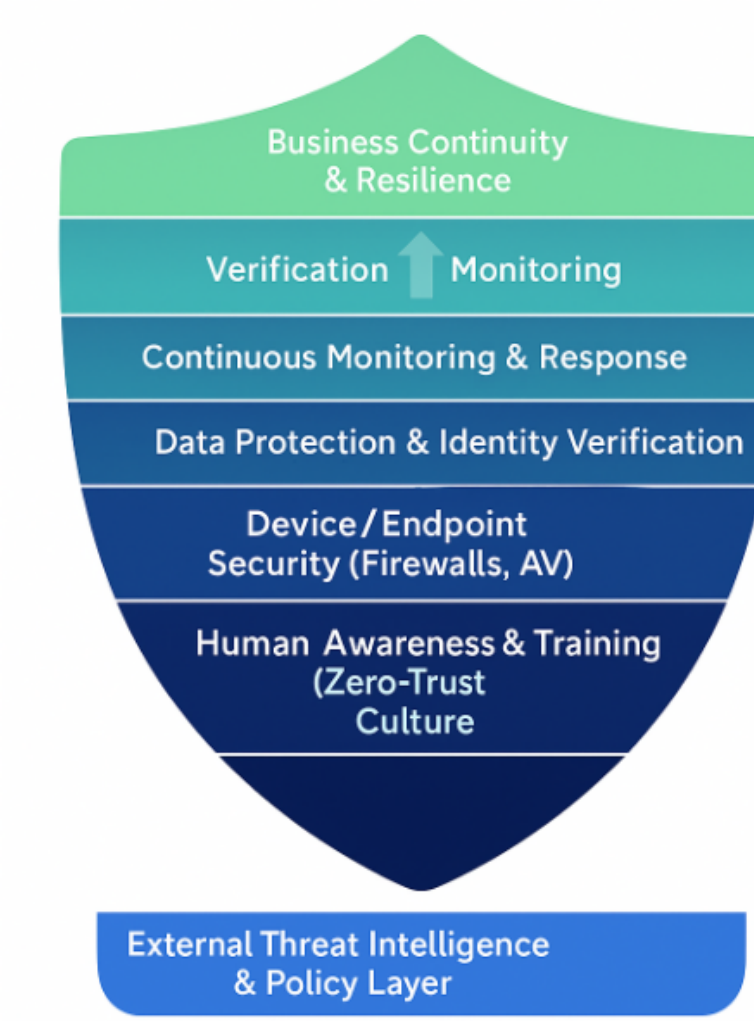

Figure 5-1: Layered Defense and Zero-Trust Approach Model for SMEs in Abu Dhabi. Source: author-developed model.

Figure 5-1 shows the suggested Layered Defense and Zero-Trust Approach Model, which is an integration of the Defense-in-Depth strategy and the Zero-Trust Architecture (ZTA) principle to enhance the Information Security Management (ISM) in the small and medium enterprises (SMEs) of Abu Dhabi. The model proves the effectiveness of multi-layered protective measures and continuous verification in

improving the resilience of an organization to emerging cyber threats (Kindervag, 2010; Rose et al., 2020; Shackleford, 2019).

The External Threat Intelligence and Policy Layer is placed at the base and reflects the regulatory and strategic climate to ensure adherence to the UAE cybersecurity requirements (UAE Cyber Security Council, 2022). The Human Awareness and Training Layer emphasizes that employee education and a culture of never trust, always verify, is the primary point of defense (Aldawood and Skinner, 2018). The new elements are introduced with Device and Endpoint Security providing firewalls, antivirus software, and updates, Network Security and Micro-Segmentation reducing lateral movement by isolating devices and filtering traffic (Whitman and Mattord, 2021).

There is an Access Control and Identity Verification Layer, which implements least-privilege and multifactor authentication, as well as Data Protection and Encryption that maintain confidentiality and integrity (Peltier, 2016). On top of them, Continuous Monitoring and Response allows detecting and responding immediately (NIST, 2020; CISA, 2021). First in the list, Business Continuity and Resilience are the long-term operations and preparedness to recover (Bada and Sasse, 2015).

The color gradient between blue and green is used to signify the transformation between the technical protection on the ground plane to the highly advanced resilience and adaptive verification without trust. Blue represents stability, control and compliance as green represents growth, flexibility and maturity. Such a visual transformation is an indication of SME moving past affordable baseline security controls into a comprehensive digital resilience approach within a Zero-Trust ecosystem (Rose et al., 2020; UAE Cyber Security Council, 2022).

5.6 Linking themes to Protection Motivation Theory (PMT)

5.6.1 Linking Theme 1 to (PMT)

The results of the Theme 1 indicate that the adaptive security practises of the SMEs when dealing with COVID-19 are clearly aligned with the constructs of the Protection Motivation Theory (PMT). The participants exhibited an enhanced threat appraisal by showing a greater understanding of escalated severity and vulnerability of cyber-risk when operations moved to the online space (P01, P03, P06, P12). This knowledge on the vulnerability to ransomware, phishing, and remote-access, led to proactive coping strategies. The focus on implementing Zero-Trust frameworks and layered security improvements (P01, P02, P10, P14) can be seen as an example of response efficacy, with companies being confident that security technologies would help them overcome the emerging threats. Equally, allusions to cloud migration and VPN usage (P07, P08, P16) represent an evaluative belief that technological defences are effective and warranted to sustain resilience in the conditions of remote-work. Self-efficacy was also reflected in some participants as they explained how already existing protocols and internal abilities

helped them easily switch to secure digital operations (P05, P11, P19). These coping appraisals highlight the belief of SMEs in their own ability to deal with security threats despite the scarcity of resources. Moreover, some participants also admitted the expenses of responses like higher financial expenditure to maintain a sufficient level of protection but they were presented as valuable trade-offs in order to minimise exposure (P01). All these findings support the conclusion that post-COVID security adaptations of Abu Dhabi SMEs are strongly anchored in cognitive risk and ability appraisals as hypothesised by PMT and demonstrate a balanced combination of perceived severity, coping efficacy, and adaptive motivation in the process of developing information-security behaviour.

5.6.2 Linking Theme 2 to (PMT)

The history of the digital uptake of SMEs in Abu Dhabi reflects a behavioural change that is long-lasting and meets the cognitive construct of Protection Motivation Theory (PMT) in many ways. Respondents reported how the pandemic triggered a long-term transition to safe digital ecosystems - especially via cloud migrations, remote working infrastructure and Zero-Trust settings - as a response belief of strong response efficacy and self-efficacy (P01, P02, P05, P07, P08, P10). These testimonies show the optimism of the efficiency of digital solutions and internal resources to uphold operational and information safety levels. The participants also admitted that the security needs were constantly evaluated, and an iterative coping appraisal process was suggested, balancing the perceived threats with the confidence in the protective measures (P03, P04, P17, P18). Indicatively, the long-term investment in cyber security tools and infrastructure upgrades indicate that SMEs view the measures as plausible to minimise vulnerability and increase resilience. The sensations of constant watchfulness and reinforced security stance also indicate the perceived severity and threat cognizance, in which the perception of cyber risks still influences future proactive security behaviour (P11, P12, P15, P19). In general, the results indicate that the impact of digital adoption goes beyond the technological shift and represents a psychological shift in the security attitudes of SMEs. This change concurs with the suggestion of PMT that protective behaviours are maintained when the individuals and organisations not only perceive threats but also believe in their effectiveness and ability to react effectively.

5.6.3 Linking Theme 3 to (PMT)

The results of this theme indicate that there is a high correlation between the implementation of information security practises by the Abu Dhabi SMEs and the cognitive processes suggested by the Protection Motivation Theory (PMT). Efficacy of response was represented by the introduction of high-tech monitoring tools, multi-factor authentication, and firewalls and participants expressed confidence that such technical features could effectively prevent cyber risks (P01, P02, P03, P07, P10, P17). The active focus on the active upgrades of the systems, such as the incorporation of endpoint protection and

safe cloud environment, indicates that the participants trust the effectiveness of the technological protection against the threat of sensitive information disclosure. At the same time, frequent awareness campaigns among employees and compulsory security training also depict self-efficacy since SMEs believed that their employees could recognise and react to the threats that appeared (P04, P08, P11, P12, P13, P19, P22). The perceived severity and vulnerability were increased due to experiences of phishing attacks and ransomware incidents, which prompted organisations to adopt layered defence controls and improve incident response plans (P16, P18, P23). The readiness to invest in upgrades of the system and continue regular training despite the limited finances can be seen as coping appraisal, which is a continuous assessment of the balance between the benefits of protection and the costs (P09, P25). Taken together, these practises are a sign of an adult level of security stance, which combines technical solutions with human consciousness, supporting the statement of PMT that a long-term protective motivation can be achieved by a combination of the perceived threat seriousness and the belief in the ability to react to threat. The theme therefore highlights how the post-pandemic ISM frameworks of SMEs are not reactive but strategically based on cognitive judgments of risk, control and efficacy which reflect the theoretical architecture of PMT.

5.6.4 Linking Theme 4 to (PMT)

The results of Theme 4 show that the resource and capacity issues that SMEs in Abu Dhabi experienced during and after the pandemic can be well explained using the Protection Motivation Theory (PMT). The participants emphasised financial limitations, lack of technical skills, and reliance on third-party providers as the main barriers to maintaining a comprehensive security framework (P01, P04, P05, P14, P18). These obstacles are based on the response cost in which a perceived cost and perceived complexity of the implementation process are determinants of the desire to adopt or upgrade information security. However, various SMEs were characterised by high coping appraisal through maximisation of available tools, consolidation of IT roles and use of cloud-based services to limit resource constraints (P03, P07, P10, P19, P22). It shows an assumption that the low-cost or incremental security measures are effective when properly positioned- a major aspect of response efficacy. The increased sensitivity to the possible breaches, phishing, and insider threats also indicate the presence of strong threat appraisal, as the participants were aware of the gravity of cyber-related threats but had to do what they could (P11, P12, P17, P20). Besides this, ongoing employee education, despite small budgets, is also a long-term self-efficacy that demonstrates that SMEs are confident in the ability of their employees to react adequately to the security issues (P09, P15, P23, P25). On the whole, this theme emphasises how SMEs can find their way at the crossroads of limited resources and increased risk perceptions which confirms the assumption of PMT that successful protection decisions are the results of a dynamic equilibrium between perceived severity, coping capacity and practical resource assessment. The data confirm that

adaptive resilience of SMEs is not based on the resources but informed appraisal procedures that facilitate sustainable and context-specific ISM practises.

5.7 Explaining SME Behaviour under PMT and Digital Resilience Theory

The behavioural tendencies observed among Abu Dhabi SMEs during and after the COVID-19 pandemic can be better understood through the combined explanatory lens of Protection Motivation Theory (PMT) and Digital Resilience Theory. PMT clarifies the cognitive mechanisms behind security-related decisions, while resilience theory highlights organisational adaptation and recovery dynamics in the face of digital disruptions.

From the PMT perspective, SME managers' actions reflected strong threat appraisal—a heightened awareness of cyber risks and vulnerability arising from remote work, cloud migration, and increased digital exposure. Participants' frequent references to ransomware, phishing, and data-loss concerns demonstrate an internalised perception of severity, motivating preventive measures. Simultaneously, coping appraisal-confidence in the effectiveness of adopted technologies and self-efficacy in managing risks-shaped decisions to invest in layered defence systems, firewalls, and zero-trust frameworks. Thus, SMEs acted not simply in reaction to external pressures but through a rational, psychologically anchored evaluation of threat and capability.

Complementing this, Digital Resilience Theory explains how these behavioural patterns evolve beyond immediate protection toward long-term adaptability. SMEs displayed resilience by transforming security into an enabler of continuity, leveraging digital infrastructure for remote operations, cloud-based recovery, and employee training. This behaviour illustrates an emergent form of anticipatory resilience, where prior experiences of cyber incidents or operational stress informed proactive investment in security culture and redundancy mechanisms.

Overall, SMEs behaved as adaptive, learning entities whose cybersecurity choices were driven by a dual logic of protection motivation and resilience building. Their behaviour was not purely reactive but strategically oriented toward maintaining operational stability and competitive viability in uncertain digital environments. This integration of PMT and resilience theory underscores that SME responses are guided by both perceived vulnerability and the desire for long-term digital sustainability.

CHAPTER 6: CONCLUSION

6.1 Introduction

The main purpose of this dissertation was to critically unravel the effect and legacy of COVID-19-related digital adoption on the ISM practices of Small and Medium-Sized Enterprises SMEs operating within Abu-Dhabi. Focused on the Protection Motivation Theory, which postulates that protective behaviour is basically driven by individual's perception of threats and their coping appraisals, this research is focused on revealing the way in which SMEs have adjusted their ISM practices in response to increased cyber threats from the pandemic. In this respect, the study adopts a qualitative case study design by relying on semi-structured interviews with SME executives and cybersecurity experts to capture subtle changes in ISM practices that result from accelerated digital adoption. The findings reveal that SMEs in Abu Dhabi have gone through remarkable changes in ISM practices during COVID-19, driven by the necessity for operational continuity, spearheaded through increased work-from-home capabilities and necessitating cybersecurity. These results have been summarized and discussed within the larger context in an effort to provide actionable recommendations for both SMEs and policymakers on the manner in which ISM resilience can be enhanced in a post-pandemic scenario.

The overnight thrust on digital platforms made SMEs open to a whole bunch of security threats. Enterprises were now more susceptible to advanced phishing scams, ransomware, and DDoS attacks. Added to these were increased reliance on third-party cloud service providers and the work-from-home policies that ensured a particularly topsy-turvy security environment. This has seen SMEs embrace a number of security measures. Among them was the deployment of multi-factor authentication and integration of cloud-based security solutions. It also included engagement in regular cybersecurity training for employees. All these activities were prone to see their effectiveness grossly curtailed by the crippling financial and general technical expertise pitfalls.

These findings consequently provided strong support for the Protection Motivation Theory (Jamil et al., 2024; Sulaiman et al., 2022), since it suggested that the heightened perception of cyber threats due to the pandemic had indeed motivated SMEs to improve their ISM practices. This theory identifies perceived severity and vulnerability as the key motivators in adopting protective behaviour. Conclusions derived from these findings show that SMEs operating in Abu Dhabi cannot afford to underestimate the value of sophisticated ISM practices as an integral component of their overall digital transformation process. Courses of actions that are recommended: Impart continuous education and training programmes so that all employees can be made aware of the different ways by which cyberattacks occur and what response approaches are applied in an effective way.

In that respect, SMEs should be encouraged to invest in state-of-the-art security technologies, including AI-driven ones able to anticipate and neutralize threats before they have the chance to make their move. In this regard, it is necessary for SMEs to introduce and continue improving comprehensive ISM policies in all aspects concerning security and ensure timely reviews of such policies to maintain concurrency with the best practice in security matters and updates in technology. Clearly, much is to be gained by encouraging closer cooperation between SMEs and between SMEs and larger enterprises by sharing best practice, experience, and strategy that deal with how to manage ISM in the digital economy. Creating forums or working groups to give special attention to issues related specifically to cybersecurity for the SME sector would above all prove to be particularly useful.

Based on these issues, the policymakers should implement some strategic steps to save SMEs, as these are important parts of Abu Dhabi's economy and, obviously vulnerable to cybersecurity threats: Providing tax breaks or subsidies as incentives for financially aiding SMEs to develop and implement proper cybersecurity infrastructures. Strengthen the regulatory regime that governs digital security with focused guidelines and standards relevant for SMEs, aimed at creating a clear road map for compliance. Increase funding towards cybersecurity research oriented in developing security solutions which are affordable and suitable for SME needs. Promote public-private partnerships to utilize the know-how and resources of large enterprises and government agencies to help SMEs improve their cybersecurity.

This has been instrumental in showing that the COVID-19 pandemic acted as an accelerant for this adoption of digital among Abu Dhabi SMEs, which has greatly transformed their Information Security Management practices. These changes created different new challenges but spurred innovation and strategic shifts in how SMEs manage information security. These experiences can, therefore, help SMEs in their efforts toward better preparation against future challenges, ensuring their operations will be protected from cyber threats and they will keep on thriving in a more digital world. The recommendations provided in this study are hence purposed to support SMEs in these efforts and help them take part in fostering a safer and resilient digital ecosystem for the protection of all stakeholders.

To make the discussion of how this study relates to different focal areas clear and systematic, a summary of the contributions is provided in the following table. These contributions are in accord with the research objectives outlined in Chapter 1 and evidence the theoretical, knowledge, and practical progress made through this research.

Table 6-1: Summary of the Findings

Focal Area	Study Contribution
Theoretical Contribution	Developed PMT in the context of SMEs and underlined its importance in the context of the resource-scarce environment of Abu Dhabi. This adaptation focuses on how SMEs adopt ISM practises based on perceived cyber threats and coping during crises.
Knowledge Contribution	SMEs in Abu Dhabi were found to have certain distinct Cybersecurity issues in post-COVID digital transition: financial constraints, reliance on third-party vendors, and remote work vulnerabilities. Therefore, this research contributes to the existing literature by identifying how SMEs manage to cope with the fast pace of digitization in emergent economies.
Practical Contribution	Produced a best practise model and a set of concrete and specific SMART recommendations for SMEs. These recommendations cover both short-term and long-term ISM solutions including integrating multiple layers of security, raising awareness on cybersecurity through training and improving cloud security management.

This research contributes to the development of the PMT by testing it on SMEs in a regional and crisis context. Unlike previous studies that target either large organisations or individuals' security behaviours, this work shows how external factors, including the COVID-19 outbreak, influence SMEs' protective actions, including implementing sophisticated ISM safeguards. The results also highlight the importance of resource limitations and organisational behaviour in determining ISM practises and enhance the knowledge of PMT in a practical and theoretical framework.

This research offers essential information security management findings for SMEs in Abu Dhabi via qualitative case studies. It explains how certain risks, including restricted funding, dependence on external cloud solutions, and protecting remote employees, affect SMEs' cybersecurity posture. Therefore, situating these challenges in the socio-economic context of Abu Dhabi, the study provides new insights into the topic of SME cybersecurity in the global context, especially with respect to emerging economies.

The study is useful because it provides SMEs and policymakers with a best practice model and SMART recommendations. For instance, the model prescribes the layered security measures, customised cybersecurity awareness campaigns, and the use of relatively inexpensive but adequate ISM tools. These contributions are to assist SMEs to manage risks, enhance resilience, and ensure the continuity and stability of secure digital environments for SMEs, which are in line with the general objectives of enhancing the safety and reliability of the SME sector.

6.2 Addressing the Research Aim and Objectives

6.2.1 Information Security Practices' Evaluation

The research objective was 'to critically evaluate the practices of information security in SMEs in Abu Dhabi in the post-COVID-19 pandemic', and this study discusses with clarity the changes that have occurred in this SMEs sector in information security practices, from development to refinement.

Most significantly, the shift towards more sophisticated security infrastructures by SMEs is continued, despite the challenges posed by the pandemic. This change is being carried out through the adoption of cloud-based solutions that allowed flexibility and scalability, increasingly in demand. These solutions have been instrumental in the process of enabling SMEs to rapidly adjust their operational capacity with minimal disruption during fluctuating demands for and requirements of remote work. A move to cloud-based platforms has meant not only easier access and management of data but also that the SMEs have become resilient against disruption by storing and processing data in a decentralized manner.

This has been coupled with the increased effort on the improvement of endpoint protections. The shift to working remotely heightened the need to protect endpoints, consisting of personal and company-issued devices accessing corporate networks from different, often less secure, networks. SMEs have increasingly adopted advanced endpoint security controls, which include sophisticated antivirus applications, firewall protections, and multi-factor authentication mechanisms. These steps are all crucial in preventing malware, phishing, and other forms of cyberattacks; most of these have increased in frequency and sophistication with the pandemic.

These updated information security practices have been approached in great detail in the research, providing a clear view of the information security environment currently characterising the sector of Abu Dhabi's SMEs. The analysis shows not only the adoption of new technologies and strategies but also the overall enhancement of information security awareness by SMEs. It underlines the strategic importance attached to information security for business continuity and sensitive data protection against the COVID-19 pandemic threat landscape.

The information security management by the SMEs in Abu Dhabi after COVID-19 shows much progress, preliminary toward a more robust and mature information security framework. A move to the cloud and strengthening endpoint protections represent proactive efforts regarding the new normal with increased remote operations and increased cyber threats. These combined measures support creating a more resilient SME sector, enabling it to safely deal with the complications that arise from a business environment affected by the pandemic. Indeed, the knowledge emanating from this research affirms that considerable digital initiatives have been taken by the SMEs themselves, emphasizing the key role they represent within the wider economic infrastructure of Abu Dhabi.

6.2.2 Conceptualization of Problems of Information Security

The second objective of this research was to conceptualize how SMEs in Abu Dhabi address information security challenges during times of the COVID-19 pandemic. The study indeed has provided insight into the complex challenge faced during this time, largely as an outcome of the rapid digital effort and adjustment to new working ways.

A big complication indicted by this research was that SMEs relied more on the provision of services externally, especially cloud services, resulting from the pandemic. This makes it challenging for SMEs in exposure to the security protocols and practices of the third-party providers. If the providers happen to fail in maintaining high standards of security due to operational challenges or serious security threats, SMEs are more likely to encounter data breaches and service disruptions. This also becomes more acute with the providers who are facing operational challenges or serious security threats, which may affect all the dependent SMEs in a cascading way.

Besides this, financial limitations were also observed in the study as one of the major impediments to the improvement of information security frameworks in SMEs. The onset of the pandemic coincided with a time when there was an increasing requirement for heavy investments in information security infrastructure, falling along periods of economic contraction that reduce available budgets and force many SMEs to make immediate decisions about survival in preference to long-term security improvements. Further, because of this factor, financial pressure barely allows SMEs to afford state-of-the-art security technologies or even qualified information security professionals, making them more easily exposed than big enterprises with much deeper pockets.

Another critical challenge that emerged from the research is the logistical complexities associated with managing security in a remote work environment. The shift to a remote working environment has placed pressure on SMEs to rapidly adapt their security practices to protect remote endpoints and secure data communications across probably insecure networks. This situation necessitates the deployment of virtual private networks, enhanced endpoint security solutions, and access controls. Indeed, to achieve

this universally and effectively in a dispersed workforce poses quite substantial logistical challenges and resource commitments.

Moreover, the findings of this study give a complete perspective of the information security challenges faced by SMEs in Abu Dhabi during their digital transformation, considering the context of the COVID-19 pandemic. This study provides a deeper overview of critical issues like dependency on external service providers, financial constraints, and logistical challenges of managing remote work security to frame these struggles within the broader context of ISM. These are key insights into current security needs, which could also provide a basis for the development of strategies that might help mitigate these challenges in the future. Thus, this conceptualization forms a basis for further work on enhancing the information security resilience of SMEs within the region.

6.2.3 Identification of tools and solutions

The identification and assessment of tools and solutions that address information security challenges faced by the Abu Dhabi SMEs during the adopting COVID-19-related digital practices represent the successful completion of the research objectives. The present research identified several strategies, which were either technical or administrative, that the SMEs used to negate the challenges ushered in by the pandemic.

Significant attention was given to how SMEs made use of technological solutions within this emerging landscape of cyber threats. In this respect, protection services against DDoS were very important. Essentially, a DDoS attack overwhelms systems with internet traffic on a very large scale, bringing the digital operations of a company to a grinding halt; a consequence that has increased with the rising online presence of business operations. These services block SMEs from DDoS attacks, thus ensuring the continuity and availability of online services, which have become quite important for business operations during the pandemic.

The study also investigated the adoption of DLP systems; these are very important in ensuring sensitive information cannot be lost, misused, or accessed by unauthorised users. Such securities are crucial, since all businesses are increasingly relying on digital channels as a means of carrying out their operations, thereby exposing sensitive data to newer vulnerabilities.

From an administrative perspective, some of the main solutions that the study emphasised on the human factor in information security were increased information security awareness training. With remote work becoming mainstream, employees needed training on the security vulnerabilities remote operations might face and how best to mitigate such risks. Regular training will help avert the risk from potential security breaches that could come from human error by developing a knowledgeable workforce who can recognize a potential security threat and take appropriate action.

The study presented how robust information security policies are able to define and guide the handling of sensitive information, the response to security incidents, and adherence to security practices. Essentially, the important policies in setting up clear guidelines on action upon an instance of a cyber-incident are those that provide for consistency in keeping up with best security practices.

By examining these technological and administrative tools and solutions, the study furnished comprehensive evidence for all current approaches employed in securing digital infrastructures from evolving threats. It is this kind of comprehensive analysis that puts the effectiveness of these measures into context but at the same time also gives a lead for other SMEs to reinforce their information security strategies in response to the digital challenges posed by the COVID-19 pandemic. The insights derived are of utmost importance to SMEs in their effort to enhance their information security posture and will also be of value to those policymakers concerned with the support of business digital security in the region.

6.2.4 Best Practice Model Development

The fourth research objective is to critique options for addressing SME cyber challenges and develop an associated model for best practice, which has been comprehensively achieved. This included a detailed analysis of the challenges and solutions that are currently being employed by SMEs in the post-COVID-19 context and was synthesised into a structured model that encapsulates effective strategies for ongoing information security enhancement.

This best practice model is an outcome of detailed research and analysis, integrated with the insights gathered from studying SMEs in Abu Dhabi. These insights included identification of some of the key challenges facing the firms in the region, such as dependency on external service providers, financial constraints, and logistics of managing security for a remote workforce. Thus, the model frames recommendations that are tailored to the realistic conditions and limitations of SMEs in regard to the specific challenges addressed.

It is a practical, multi-layered approach that the model of security is workable and adaptable for implementation by SMEs with a view to enhancing information security measures. The technological defences range from advanced firewalls to DLP systems, while administrative strategies include continuous information security training and the development of relevant policies. Such a multi-layered approach ensures that the measures taken are strong, covering potential vulnerabilities at various points of possible exposure.

While this model has been founded on localised findings in Abu Dhabi's SMEs, it also considers best practices in information security from the global perspective. This is important, for it ensures that such recommendations are not only relevant but also current to the international standards and best

practices. The model considers the global scope of cyber threats and the interconnectivity in digital technologies; hence, it had to be important for businesses not only at the local scene but also for regional businesses in similar markets.

The model presents an actionable plan that SMEs follow to manage their information security posture, in a seamless way addressing identified and agreed-upon steps and measures, that may be adapted to meet particular needs and capacities of every single SME. The model shall help SMEs through a structured yet flexible approach that allows priority attention regarding the most critical vulnerabilities and available resources.

In other words, the aim to develop a best practice model aimed at addressing SME cyber challenges was not only reached but performed and accomplished in such depth of understanding and practical insight. This model testifies to being well-researched and thoughtful construction framework that could enhance information security practices not only in Abu Dhabi but also beyond. It calls for continuous scanning and adaptation, something quite relevant in the rapidly changing area of information security, to keep SMEs resilient against the threats they continuously face while growing and innovating in their respective industries. As illustrated in Figure 6-1, the proposed ISM Framework integrates digital resilience principles and protection motivation constructs to enhance SME cybersecurity preparedness in Abu Dhabi.

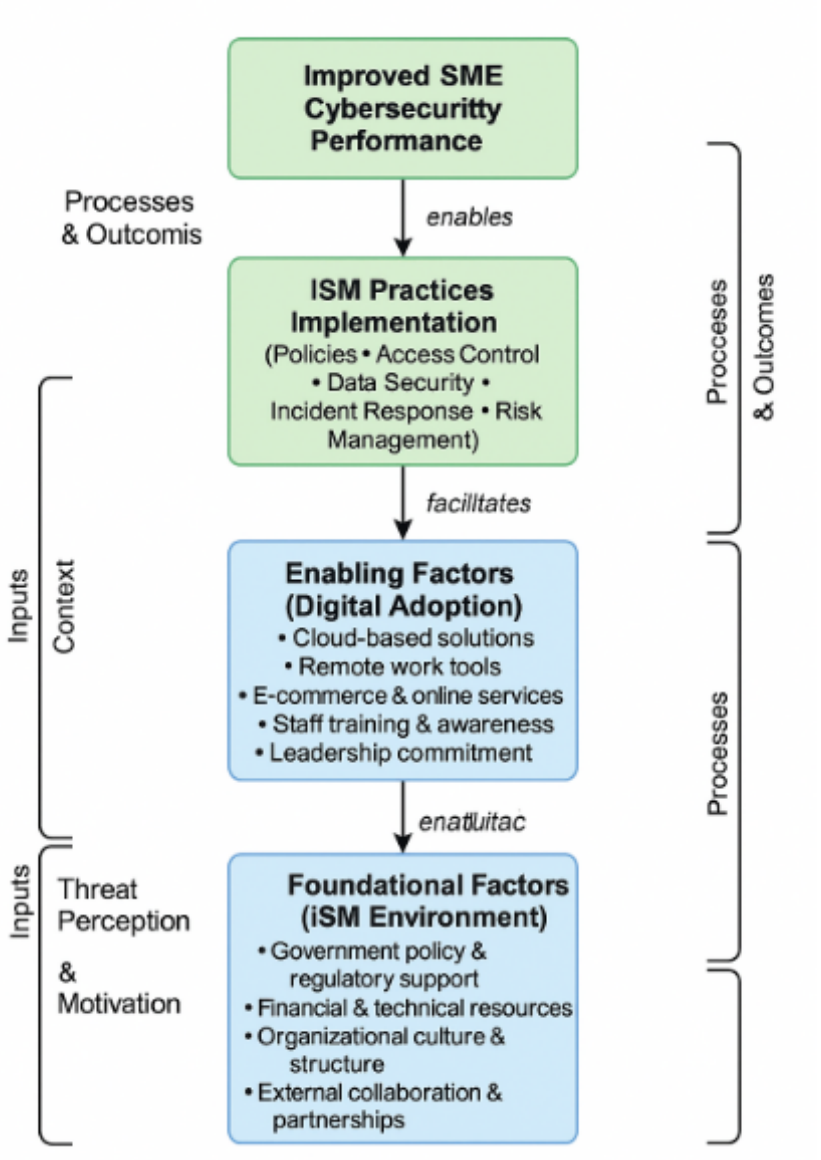

Figure 6-1: Proposed ISM Framework for SMEs in Abu Dhabi.

Source: (Author-developed framework based on study findings)

Figure 6-1 illustrates the Proposed Information Security Management (ISM) Framework designed for small and medium enterprises (SMEs) in Abu Dhabi. The framework integrates empirical insights from the study with established theoretical foundations, primarily Protection Motivation Theory (PMT) and Digital Resilience Theory, to provide a structured model for strengthening cybersecurity capability (Rogers, 1983; Whitman and Mattord, 2021; Rose et al., 2020).

At the base, the Threat Perception and Motivation Layer represents the cognitive dimension of ISM, where SME managers' perceived severity, vulnerability, and efficacy beliefs determine proactive engagement in security behaviours (Bada and Sasse, 2015; Rogers, 1983). Above this, the Foundational Factors (ISM Environment) layer captures institutional and contextual enablers, including government

regulation, financial resources, and organisational culture that shape the security climate (UAE Cyber Security Council, 2022).

The next level, Enabling Factors (Digital Adoption), highlights operational facilitators—such as leadership commitment, staff training, and adoption of cloud-based technologies—that strengthen an organisation's digital capacity and readiness (Ahdadou et al., 2022). These directly support ISM Practices Implementation, where operational measures like policy enforcement, data protection, risk management, and incident response are executed to ensure cyber resilience (Peltier, 2016; Shackleford, 2019).

The uppermost level, Improved SME Cybersecurity Performance, represents the desired outcome, reflecting an SME's ability to maintain secure, resilient operations amid emerging threats (NIST, 2020; Rose et al., 2020). The vertical sequence of relationships—"enables" and "facilitates"—demonstrates a logical progression from perception and capability to implementation and outcome.

The blue-to-green gradient visually signifies the evolution from foundational awareness (blue) to strategic maturity (green). Blue symbolises stability, compliance, and preparation, while green denotes growth, adaptability, and sustained resilience, illustrating SMEs' transition from security readiness to holistic ISM excellence (Kindervag, 2010; UAE Cyber Security Council, 2022).

6.3 Research Questions Revisited

The main research questions explored in this research were:

1. How has the digital adoption driven by COVID-19 impacted information security management practices in SMEs in Abu Dhabi?

2. What strategies, tools, and frameworks can effectively address the cybersecurity challenges faced by SMEs in Abu Dhabi during the COVID-19 digital landscape?

6.3.1 Impact of COVID-19-Driven Digital Adoption on Information Security Management Practices in SMEs

The first research question aimed at determining the impact of covid-19-driven digital adoption on information security management practices in SMEs. When compared with the research findings, it can be concluded that the increased digitization due to the COVID-19 pandemic significantly impacted ISM practices in SMEs in Abu Dhabi. The outbreak of the global pandemic led to the enhancement of the digital environment, work from home policies, and the use of cloud solutions to continue business operations. However, this rapid shift also exposed a lot of changes in SMEs' cybersecurity approaches, as they faced new and more complex cyber threats while striving to protect their digital assets with

limited resources. This study established that this increased digital adoption had both benefits and risks as SMEs had to implement different cybersecurity measures, which were mostly done in a reactive manner, to protect business activities and information.

Among the direct effects of digitalisation, it is necessary to identify the growth in the number of the identified cybersecurity threats, including phishing attacks, ransomware incidents, as well as data breaches. Small and medium-sized enterprises, which had little to no cybersecurity measures in place, left themselves wide open to cybercriminals to penetrate their systems. This work established that SMEs reacted by strengthening their security frameworks, which was largely reactive in nature. This is in a way supported by the Protection Motivation Theory (PMT) which postulates that perceived risk and threat magnitude dictate protective action. Due to the increased risks that were associated with financial transactions, business secrets, and customer data, SMEs started using firewalls, antivirus, and simple encryption. Nonetheless, most of the SMEs faced problems by having limited knowledge, skills and funds in cybersecurity, thus, they had limited protection and lacked in the application and implementation of sophisticated security measures.

As the business moved to cloud environments, the SMEs relied on the third-party cloud service providers for the storage and management of their data. Although cloud technology had some advantages like flexibility, affordability, and accessibility, it brought new challenges to security. The research conducted showed that most of the SMEs had little knowledge about shared responsibility models that define the distribution of security obligations between the Cloud Service Provider (CSP) and the customer. This lack of awareness resulted to the emergence of governance gaps, where SMEs relied on their cloud providers to provide them with security solutions, without realizing that they failed to cover aspects such as access control, data encryption, and security audits among others. Moreover, the integration issues between the old and new systems that were implemented with the use of cloud solutions led to the exposure of security threats such as unauthorised access, leakage of data, and improper configurations of the systems. This research found out that to date, the SMEs still face the risk of breaches due to the lack of a concrete cloud security plan pointing to a lack of structure in the security governance.

Another factor revealed in the research study was the lack of funds that limited SMEs from adopting proper ISM solutions. Since most SMEs could not afford to have a dedicated budget for cybersecurity, they lacked the resources to build robust security systems. A number of SMEs were unable to invest in Intrusion Detection System (IDS), advanced encryption technologies, and endpoint security tools even though they acknowledged the significance of cybersecurity. Due to financial constraints, SMEs had to focus on the urgent needs of the company's operations and could not afford to invest in long-term security solutions that would give a more robust security measure than the basic tools that were readily

available. This is in line with other studies which noted that SMEs in developing economies including the UAE are challenged by financial constraints that prevent them from developing robust cybersecurity measures. The study implies that in the absence of adequate funding or cheap solutions that are specific to SMEs, many companies will remain at the mercy of cyber criminals due to constraints in resources.

The change of working from home during the pandemic worsened cybersecurity issues, and it became a list of challenges for SMEs. Use of company networks from home environments that are not secure greatly enhanced the probability of data leak, unauthorised entry, and cyber invasion. This forced SMEs to adopt MFA, VPNs, endpoint security solutions among others to mitigate these challenges. However, many of these measures were not enough since most SMEs had no proper remote work security policies in place, which exposed them to various risks like social engineering attacks, phishing scams, and human errors. Also, there were no effective training programmes for employees on cybersecurity, and most of the staff was not knowledgeable about how they could protect company information while working from home. This is an indication that SMEs should not only invest in security technologies but also incorporate regular training programmes for the employees to ensure they are knowledgeable enough to identify security threats.

It also examined the challenges that SMEs experienced in dealing with multiple and complicated cybersecurity regulations and standards in Abu Dhabi. Companies had to ensure that their ISM practices complied with legal requirements like the National Electronic Security Authority (NESA) guidelines for organisations based in the UAE and the General Data Protection Regulation (GDPR) for organisations dealing with customers' information across the globe. However, the study established that due to inadequate skills in cybersecurity, compliance was difficult for most SMEs, and they sought the services of consultants to help them meet compliance standards. Thus, the research indicates that enhanced, SME-oriented cybersecurity rules and better guidance from the relevant authorities can contribute to enhancing SMEs' cybersecurity readiness. Without such specific guidelines that would be helpful for SMEs, the companies may still be in a dilemma on how to adhere to the requirements and avoid the consequences of legal actions.

Nevertheless, the study established that after the pandemic, there was a change in the ISM practices whereby SMEs transitioned from an isolated approach to cybersecurity to more systematic practices. The study established that an increasing number of SMEs are adopting Zero Trust security models, which is a security model that does not trust any user or device without first checking its identity. Due to the restriction of user rights according to their job responsibilities and constant check of security entrances, the probability of internal threats and unauthorised users was minimized by the Zero Trust frameworks. Finally, there was increased awareness in SMEs towards cybersecurity training where some of the businesses had integrated training sessions to update the employees on the new security threats and

measures. Other important trends included cybersecurity audits and penetration testing, which were also adopted by SMEs for maintaining a culture of risk management as opposed to threat management.

In conclusion, the COVID-19 has accelerated the change in ISM practices among SMEs in Abu Dhabi and the changes have become permanent. Although digital transformation helped SMEs to continue operations, it also led to an increased level of cyber threats that pushed companies into reviewing their security posture, improving the security and adopting new technologies. As it has been established, cloud solutions, remote work models, and digital platforms became crucial for the SMEs' operations, they also brought new risks that most companies were not ready to face. Lack of funding, dependence on external suppliers, and insufficient knowledge of cybersecurity issues became the key challenges to ISM implementation. Nevertheless, the results show that SMEs are gradually waking up to the reality of cybersecurity and are gradually adopting better security management, regulation, and constant training of employees. In the future, the SMEs should be provided with more financial assistance, specific guidance on compliance with the laws, and affordable security solutions to continue to improve the cybersecurity in their businesses in the context of the increasing use of digital technologies.

6.3.2 Strategies, Tools, and Frameworks for Addressing Cybersecurity Challenges in SMEs

The second research question focused on identifying best practices, solutions and frameworks that may help the SMEs mitigate the challenges that they encountered during and after the COVID-19 crisis. The research results indicate that SMEs used a wide range of security strategies that involved technical solutions, compliance with the rules and regulation and the best security practices. Due to the financial and technological limitations, SMEs only able to implement cost-effective yet effective measures to secure their information technology assets against cyber threats.

One of the key cybersecurity strategies that were established in this study was the implementation of security tools to improve the functionality of ISM. As for the IT security, the surveyed SMEs in Abu Dhabi enhanced the usage of various protective mechanisms to protect the networks from unauthorised access. Some of the tools used included firewalls and endpoint protection tools which acted as the initial barrier to the cyber threats by blocking traffic that was deemed unsafe and preventing any device on the company network from getting infected with malware. Another widely implemented tool was the Multi-Factor Authentication (MFA), which involves using multiple methods of verifying a user in order to minimise the chances of a hacker gaining access to an account through stolen passwords or other similar attacks. In addition, SMEs also adopted Data Loss Prevention (DLP) systems for keeping track of, regulating, and blocking any unauthorized transfer of data in order to manage the risks of data leakage and internal threats. A few of the SMEs also adopted the Intrusion Detection and Prevention Systems

(IDPS) to control and prevent cyber threats from affecting their business operations in real-time. However, this research established that many SMEs were not well-equipped with cybersecurity training to enhance the efficiency of these tools. In addition, due to financial constraints, these security systems could not be upgraded constantly, which underlined the need to provide financial help and training to SMEs to help them make the best out of cybersecurity technologies.

Besides the use of cybersecurity tools, the awareness of the threats and risks and training of employees in cybersecurity became one of the most important factors in the SMEs' security plans. The study also revealed that human factor was still a significant threat to cybersecurity, as the employees were frequently targeted with phishing, social engineering and improper handling of data. The SMEs that adopted to incorporate routine training sessions on cyber threats and risks were able to reduce the number of cyber incidents and enhance their understanding of the threats. Some of the training areas focused in these programmes were phishing, protection of sensitive business information, and working remotely security. These training programmes were very helpful in strengthening the organisational cybersecurity culture since all employees would be able to recognize and report any possible threats. This study emphasizes that training and awareness should be an ongoing process in the SMEs since the technical measures alone cannot address all the cyber threats without the cooperation of the users.

One of the cybersecurity models that are slowly but steadily gaining popularity among SMEs in Abu Dhabi is the Zero Trust security model which is based on the concept of 'never trust, always verify.' This model makes sure that all users, devices, and applications are verified and supervised before they are allowed to connect to the business networks and resources. The study revealed that SMEs leveraging on Zero Trust frameworks received increased security measures in that they limited insider risks, prohibited cyber threats from moving from one segment of the network to another, and strengthened the identity protection mechanisms. Also, this framework helped the SMEs to compartmentalize the networks so that even if the hackers penetrated a particular segment, they could not access the other segments in the network. However, the study also showed that there are some issues that prevent SMEs from implementing Zero Trust models; these include technical challenges and the absence of cybersecurity skills within the companies. For the SMEs to implement this framework, they need to seek assistance from the outside world, technical support, and cybersecurity training to develop the required competency to implement the framework.

Since the financial and technical capabilities of most SMEs are restricted, many of them decided to delegate cybersecurity management to third-party entities. The study also revealed that MSSPs were instrumental in enhancing the security level of SMEs without the need of internal IT skills. SMEs benefited from gaining professional security services, continuous monitoring of threats, and immediate response to incidents with the help of outsourcing at a much lower cost than employing an in-house

cybersecurity team. Moreover, cooperation between government organisations and small businesses, large companies, and SMEs were deemed as the best solution to fill the gap in cybersecurity knowledge and funding. Such collaboration enabled SMEs to get cheap security training, affordable security products, and information on what measures to implement. The study also states that the enhancement of the Public-Private Partnership (PPP) would also enhance the development of SME cyber resilience as it would allow for the SMEs to tap into the knowledge and resources of large firms.

To enhance the cybersecurity posture, the SMEs synchronized their ISM practices with the international standards and regulatory requirements. The research identified that businesses in Australia and New Zealand relied on the ISO/IEC 27001 information security management systems because they helped create business management security guidelines and risk management procedures. Also, the SMEs in the UAE had to follow the National Electronic Security Authority (NESA) Guidelines that contain the cybersecurity regulations suitable for the UAE market. In addition, those SMEs operating internationally synchronized their data protection policies with the GDPR to adhere to the data privacy laws regarding customers from the European Union. But there are some challenges that were identified to affect the SMEs in their compliance to the regulatory requirements as including inadequate awareness, technical constraints and lack of human resource in cybersecurity. Specific compliance frameworks and regulatory support for SMEs would go a long way in enhancing the compliance with these standards and thereby enhance cybersecurity compliance among the SMEs.

Perhaps one of the most important recommendations that emanated from the study was the need for SMEs to ensure that they put in place well-coordinated and well-coherent incident response and business continuity policies and strategies. The findings also suggest that SMEs who had clear pre-set reaction tactics, backing up data approach, and disaster mitigation strategies implementing plans were more equipped to deal with cyberattacks and disruptions of operation. Some of the organisations that had no structured response plans incurred more time in getting back to normalcy, lost funds, and tarnished image after being attacked. In order to prevent such attacks, the SMEs were advised to undertake vulnerability assessments, practice their response plans and adopt data backup systems to enhance data security in the event of an attack. The study establishes that there is a need for SMEs to have a proper business continuity plan to ensure they can quickly recover from security breaches and have stability in the event of the cyber threats.

The findings of this study are quite strong to support the proposition that COVID-19 influenced the digital adoption of ISM practices among SMEs in Abu Dhabi. That is why digital transformation helped businesses to survive in the new environment but also brought new threats that SMEs had to counter with technical solutions, employees' training, compliance with the legislation, and proper cybersecurity frameworks. These enhanced risks led SMEs to incorporate security tools like firewalls, MFA, and IDPS,

the Zero Trust security model, and PPP for cybersecurity. However, issues like inadequate funds, skills in cybersecurity, and relying on third-party service providers were still some of the significant factors hindering the establishment of sound ISM practices.

Therefore, with the aid of proactive security frameworks, structured compliance measures as well as effective cybersecurity awareness programmes, SMEs should be able to comb their security threats problems and guarantee their business sustainability in a world that is increasingly characterized by digitalisation. The study reveals that the SMEs should adopt a multi-layered approach to cybersecurity that involves the use of technology, compliance with regulations, and training of employees. As such, in future studies should extend awareness and conduct longer-term analyses of cybersecurity measures to determine whether they can effectively address emerging challenges in the contemporary and growing context of the cyber domain.

6.4 Recommendations Based on Research Findings

This research on the state of information security among SMEs in Abu Dhabi in the post-COVID-19 period has shed light on several critical aspects of how these companies manage and mitigate cyber risks. The objectives of the research have been to assess the security practices in existence, conceptualise the information security challenges, identify relevant tools and solutions, and develop a best practice model. Detailed recommendations for improving the state of information security posture in SMEs in the region are listed below from the findings. Each recommendation is informed by the evidence in the research findings and critically examines the implications from these findings.

6.4.1 Improved Management of Cloud Security

The findings showed that there is a high dependency on external cloud service providers in the industry of SMEs, with associated risks of data being beyond reach and unavailability of customized security protocols. This dependency makes SMEs prone to vulnerabilities resulting from security breaches faced by providers themselves. SMEs should adopt more holistic cloud security management practices (Jain, 2024). This should involve the negotiation of service level agreements that detail what security measures will be put in place by the provider. A suitable response would include regular security audits and adherence to local data protection laws for example. It is also highly recommended that Cloud Access Security Brokers (CASBs) be deployed by the SMEs wherein these solutions sit between cloud users and cloud applications to monitor all activity and enforce security policies (Kunduru, 2023). This would help SMEs have better visibility and, in turn, control over the data to improve their reaction against the threats.

6.4.2 Financial Investment in Information security

The SMEs are severely circumscribed in financial resources in adopting advanced information security technologies (Armenia et al., 2021). According to the research, very often SMEs refrain from upgrades and necessary training because of costs involved in affecting their security posture. It is important that SMEs rebrand information security investment as a must-have investment rather than a discretionary investment. These incentives could be in the form of grants, tax reliefs, or subsidies to reduce the cost of information security services available to SMEs by government agencies or respective industry associations. Besides this, SMEs should look out for affordable solutions designed for SMEs that ensure scalable protection without requiring huge upfront investments.

6.4.3 Formal Cybersecurity Training Programs

The human factor remains one of the weakest points in the chain when it comes to information security. In fact, most security breaches take place due to employee mistakes or a lack of awareness of basic protection practices. More importantly, ongoing training programmes that should address general security practices, the capability of recognizing phishing and social engineering attacks, and proper handling sensitive information (Chaudhary, Gkioulos and Katsikas, 2023). This practice must be more interactive and current to face the latest information security landscape and threats. Simulated cyberattacks and drills are also worth conducting to ascertain employee preparedness for such incidents and to reinforce learning.

6.4.4 Establishment of all-inclusive information security policies

Most SMEs typically lack formalized policies related to information security, as this is of utmost importance in defining the standards and procedures concerning security within the organisation. Any existing information security policies are to be clearly spelled out with statements on comprehensive security for protection of data, incident response, and employees' responsibilities (Rawashdeh and Rawashdeh, 2023). These policies must be subjected to regular review and updates in respect of new developments in information security, as well as changes in the business line. This policy should be communicated throughout the organisation. All employees shall be required to acknowledge, in writing, the fact that they have understood and will comply with such policies.

6.4.5 Implementation of a Multi-tier security approach

The SMEs should try to implement various measures to support several layers of defence. Examples include technological measures: firewalls, antivirus software, intrusion detection systems, and administrative measures comprising tight access controls and regular security audits. Such a multi-layered approach ensures that even if one layer is compromised, additional layers of defence will guard the assets of the organisation (Manzoor et al., 2024). Therefore, the dynamic nature of the cyber threat

requires constant adaptation and updating of information security strategies. SMEs should work out procedures for regular risk assessments that would define the areas of their vulnerability and, therefore, assess the adequacy of the security measures in place. An innovative culture needs to be produced in the information security groups in the SMEs to proactively identify new threats and immediately adopt mitigation measures for them.

The aforesaid recommendations are indeed critical in their details, as they seek to guide SMEs in Abu Dhabi toward effectively strengthening their information security practices. By addressing such key matters as cloud security management, financial investment in information security, structured training programmes, comprehensive policies, a multi-layered security approach, and regular risk assessments, SMEs will be setting the stage for enhanced chances of resilience against cyber treats. These recommendations are put forward with the view to helping meet not only immediate needs but also to lay a foundation for sustainable security practices that can adapt dynamically to the ever-changing digital landscape. The implementation of the recommendations put forth in this document will enable the SMEs in Abu Dhabi to protect their critical assets and ensure business continuity in an increasingly interconnected, cyber-threatened world.

6.4.6 SMART Objectives and Recommendations

The following recommendations table presents SMART (Specific, Measurable, Achievable, Relevant, Time-bound) objectives to relate to research findings and propose relevant SMART recommendations.

Table 6-2: SMART Objectives and Recommendations

Objective	Findings	SMART Recommendation
Objective 1: To evaluate ISM practices in SMEs in the wake of COVID-19 digital adoption	SMEs adopted basic ISM practices, including firewalls and endpoint security, but lacked resources for high-end security solutions.	**Enhance Access to Affordable Security Tools**: • Partner with three cybersecurity providers within six months to create affordable security packages specifically for SMEs (Franco, Lacerda and Stiller, 2022). • Progress will be measured by the number of SMEs adopting these packages, aiming for at least 30% adoption within the first year.

	Cloud adoption facilitated remote work but increased dependency on external providers, reducing direct control over security.	**Implement Hybrid Security Models**: • Encourage SMEs to implement at least one hybrid security solution combining on-premises and cloud security for critical systems (Ali et al., 2024) within the next year. • Track adoption rates with a target of 25% of SMEs implementing a hybrid model by the end of the period.
Objective 2: To conceptualise ISM challenges in SMEs after COVID-19	Increased cybersecurity threats due to remote work and integration challenges with legacy systems were common among SMEs.	**Introduce Comprehensive Employee Training**: • Design a targeted training programme on remote work security practices to be delivered quarterly. • Each SME should aim for at least 90% participation from employees within the first six months of programme rollout, with pre- and post-assessments to measure improvement in awareness levels.
	SMEs faced technical and logistical hurdles in securing data access, leading to potential vulnerabilities.	**Promote Multi-Layered Security Protocols**: • Aim for 50% of SMEs to adopt multi-layered security measures, including encryption and multi-factor authentication, within 12 months. • Monitor progress through regular security audits conducted biannually to track adoption rates and compliance levels (Seth, Najana and Ranjan, 2024).

Objective 3: To identify solutions for ISM challenges amid rapid digital adoption since COVID-19	SMEs are financially constrained, limiting their ability to invest in advanced ISM solutions.	**Subsidized Cybersecurity Support**: • Within six months, establish a government-backed subsidy programme offering up to 50% support on cybersecurity expenses for SMEs. • Track the impact by evaluating reductions in security breaches among SMEs accessing the subsidy (Samira et al., 2024) within the first year.
	SMEs often lacked specific guidelines on ISM, which made them vulnerable to common cyber threats such as phishing and ransomware.	**Develop SME-Specific ISM Guidelines**: • Publish a comprehensive ISM guidelines document for SMEs within three months, including templates for policies and response plans. • Disseminate through industry associations, aiming for 80% awareness among SMEs and 50% adoption of at least one policy or practice within the first year.
Objective 4: To critique options for addressing SME cyber challenges and propose best practices	Social engineering attacks and human error were major security challenges, exposing gaps in ISM practices.	**Strengthen Security Awareness and Culture**: • Launch a quarterly security awareness programme with mandatory participation for all employees, aiming for 100% completion rates. • Measure effectiveness through pre- and post-training evaluations, with the goal of a 50% reduction in successful phishing attempts within the first year of programme implementation.

	Many SMEs struggled to balance operational needs with ISM priorities, impacting security efficacy.	**Encourage Minimal Access & Zero-Trust Policies**: • Establish a Zero Trust policy template for SMEs to implement (Muhammad et al., 2022) within six months, with a target of 70% adoption rate. • Conduct biannual assessments to ensure compliance and aim for a 30% reduction in unauthorised access incidents by year's end.

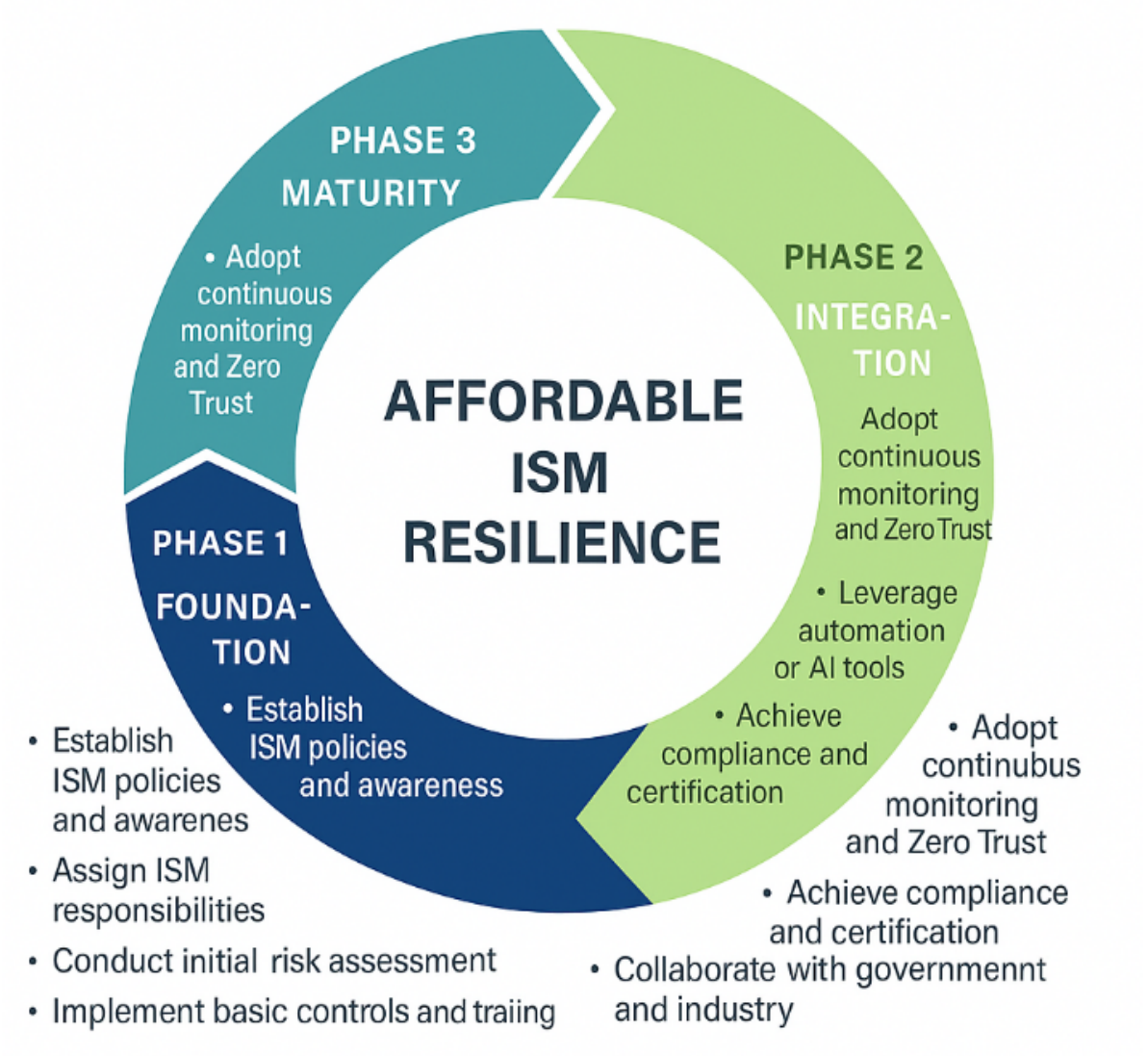

Figure 6-2: Circular Phased Implementation Roadmap for Affordable ISM Practices, Source: by author

Figure 6-2 illustrates the Phased Implementation Roadmap for Affordable ISM Practices, which operationalises the SMART objectives developed in Section 6.4.6. The model presents a continuous, cyclical process through which small and medium enterprises (SMEs) in Abu Dhabi can progressively strengthen their Information Security Management (ISM) capabilities. The circular layout emphasises that ISM improvement is not linear but iterative, reflecting the dynamic nature of cybersecurity management and resilience (Rose et al., 2020; NIST, 2020).

At the outer layer, the model comprises three progressive phases—Foundation, Integration, and Maturity each colour-coded in a blue-to-green gradient to symbolise capability development and organisational growth. Phase 1 (Foundation) focuses on establishing the basic ISM structure, including policy development, staff awareness, risk assessment, and the implementation of low-cost controls (Aldawood and Skinner, 2018). Phase 2 (Integration) advances to embedding ISM practices into daily operations, introducing cloud and remote security, enforcing access and data protection policies, and initiating compliance mechanisms (Peltier, 2016; Shackleford, 2019). Phase 3 (Maturity) represents strategic transformation, where SMEs adopt Zero-Trust measures, automate monitoring systems, and collaborate with regulators and industry peers for sustained resilience (Kindervag, 2010; UAE Cyber Security Council, 2022).

At the centre of the model, "Affordable ISM Resilience" captures the ultimate goal: achieving sustainable, cost-effective cybersecurity maturity. The circular flow visually conveys continuous improvement, knowledge reinforcement, and adaptive learning. The blue-to-green gradient further signifies the transition from foundational readiness (blue) to proactive resilience (green), demonstrating SMEs' ability to evolve from basic compliance to strategic ISM excellence (Rose et al., 2020; NIST, 2020; UAE Cyber Security Council, 2022).

6.5 Research Contribution

6.5.1 Contribution to Theory

The theoretical contribution of this study on the aspect of ISM in SMEs relates to the application of PMT in a new context: SMEs in an economically strategic and high-risk environment, such as Abu Dhabi. Conventionally, studies that have applied PMT have targeted large enterprises and individual-level ISM practices. Nonetheless, this study has demonstrated the viability of PMT in the investigation of ISM practices at SMEs.

The study unravels the psycho motivational factors behind SMEs leaders in adopting protective security practices in view of increased digital risks brought about by COVID-19. The study, therefore, further develops the application of PMT in cybersecurity challenges faced by SMEs and laid a foundation for future research studies on motivational factors that lead to the perpetuation of protective behaviour

in smaller enterprises. The study also contributes to digital adoption frameworks with the inclusion of an investigation into crisis-driven adoption within an emerging economy, where restrictions on resources and rapid digital transformation have been particularly challenging. Using this perspective, the current study develops a theoretical framework of crisis-induced digital adoption, underlining the distinctive dynamics of resource-constrained environments such as Abu Dhabi's SMEs.

Given the vital role of SMEs in the UAE economy, the present framework stipulates how forced digital transformation influences these businesses and may inform other studies on the issue of digital adoption in similar high-stakes contexts. Finally, the research links ISM with Digital Resilience Theory in a manner that roots any insight into how ISM will enhance SME adaptability and continuity in the face of cybersecurity threats. In previous studies, while many discussions on digital resiliency have been made with large enterprises and public sector organisations, the current study narrows down these discussions to SMEs to show that resilience is more relevant to smaller businesses, given their significant resource limitations.

Linked to the perspective on ISM and digital resilience, this study proposes an adaptive ISM framework for SMEs, placing them not just to resist cyber threats but to thrive in the post-COVID digital economy.

6.5.2 Contribution to Knowledge

The research extends existing knowledge through the lens of the cybersecurity landscape of SMEs during COVID-19-related digital adoption. This addresses a significant gap in ISM practices for SMEs in Abu Dhabi, where a lack of resources often undermines robust security frameworks. The study elicits insights for the security challenges and threats specific to SMEs, enhancing the ability to understand how smaller businesses might secure and maintain digital adoption.

6.5.2.1 Understanding SME-specific ISM Challenges

This research develops the knowledge base of identification of unique security challenges of SMEs in Abu Dhabi regarding their inability to autonomously mitigate cybersecurity threats due to a scarcity of resources and appropriate infrastructure. The study identifies preventive barriers to advanced ISM measures such as financial constraints, limited IT resources, and third-party dependency. The study addresses such challenges and therefore equips every business, policymakers, and researchers with relevant knowledge to design appropriate security strategies that would support the sustainability of SMEs in a digitalized landscape.

6.5.2.2 Insights for Policy and Business Practice

The study provides practical insights into SME policies and practices in Abu Dhabi and other similar regions. Well-informed policymakers can craft focused interventions that might support the

cybersecurity of SMEs. Examples include subsidised cybersecurity programmes, regulations that promote secure digital practices, and public-private partnerships focused on strengthening ISM among SMEs. In addition, by highlighting the effective tool or solution currently deployed by the SMEs in managing the threat challenges of ISM, this study is further empowering IT solution providers to shape the products and services desired for sectors' needs to ensure that digital adoption is secure and sustainable.

6.5.2.3 Widening the Discourse of Digital Resilience

The investigation of ISM in relation to digital resilience within this study provides actionable knowledge beyond cybersecurity into the wider ramifications of digital resilience on business continuity and economic recovery in the post-COVID-19 era. This study indicates how digital resilience can be enhanced by appropriate ISM practices, situating SMEs as active agents in economic resilience, especially in emerging economies. This constitutes, therefore, a broadened discussion on how digital resilience, underpinned by good ISM practice, may play a key role in the stability and development of the SME sector worldwide.

6.6 Future Research and Study Limitations

6.6.1 Future Research

This study provides a basis on which information security management could be understood in the specific context of SMEs in Abu Dhabi in the current period of rapid digital adoption. However, there are aspects that could not be covered, which could add and sharpen the findings that have been made. For further enhancing the depth and breadth of knowledge in this area, the following areas of further research could be considered:

6.6.1.1 Longitudinal Studies on Digital Adoption and ISM Evolution

Longitudinal approaches may provide a better understanding of how ISM practices evolve in the process of digital transformation, since such processes are dynamic by nature. Further research can reach sustainability and effectiveness in the ISM strategies as they adapt to new technological trends, regulatory changes, and emerging cybersecurity threats. It would be of valuable for future research to compare how crisis-driven digital adoptions, in particular, will prove more or less resilient and scalable in the longer term than voluntary, strategically driven digital transformations.

6.6.1.2 Comparative Analyses across Regions and Industries

The present study used SMEs involved in the high-growth-oriented economic region of Abu Dhabi, which is characterized by its unique landscapes of cybersecurity and related regulations. However, other studies may conduct comparative analyses between Abu Dhabi SMEs and other SMEs in emerging or

even developed regions. This can help in revealing some vital regional or industry-specific factors that may affect ISM effectiveness and subsequently suggest the development of cybersecurity frameworks tailored to suit different socio-economic contexts.

6.6.1.3 Theoretical Framework

While PMT was useful in explicating SMEs' adoption of ISM practices, future studies could embed complementary theories to represent the comprehensive landscape of behavioural, organisational, and technological factors involved. For instance, the integration of Technology-Organisation-Environment (TOE) theory can devise a broader framework by considering organisational preparedness, availability of technological resources, and environmental coercions that impact ISM adoption and cybersecurity resilience.

6.6.1.4 Quantitative Studies and Model Validation

The methodology conducted in this research is of a qualitative nature, as it allows for the determination of the specific challenges and motivations that SMEs face. A future study might apply a quantitative approach to validate the ISM framework and recommendations proposed in the current research. This could be achieved through large-scale surveys, using statistical analyses to see whether the findings of this study can be generalised to a larger number of SMEs. These approaches would further quantify the exact impact of those ISM practices on cybersecurity performance and enhance support for the application of certain measures for security in resource-limited environments.

6.6.1.5 Investigation into the Concrete Threats and Tools of Cybersecurity

This research was able to find general challenges and tools relevant to cybersecurity, used by SMEs. Still, future research may focus on specific cyber threats that dramatically affect SMEs. Meanwhile, novel ISM tools, such as artificial intelligence-driven threat detection or block chain for data integrity, would become promising in the discovery of effective resource-effective solutions for SMEs.

6.6.1.6 Impact of Policy and Regulatory Interventions

With increasing awareness among governments worldwide regarding cybersecurity and its role in ensuring economic stability, it would be worth studying the impact regulatory interventions have on ISM practices of SMEs. The effectiveness of policies such as government-backed cybersecurity subsidies for training programmes and public-private partnerships in improving the resilience of SMEs could be studied in future research. Such studies would, therefore, help policymakers understand how interventions can optimally be designed to support SMEs.

6.6.1.7 Avenues for future research

Although this research is an important contribution to the existing knowledge on the information security management practises and digital resilience of SMEs in Abu Dhabi, there are still a number of areas that can be explored in the future. To begin with, the comparative study across the GCC countries, including the UAE, Saudi Arabia, Qatar, and Bahrain, may provide a wider regional picture of the impact of socio-economic and regulatory variations on cybersecurity behaviour of SMEs. This comparative analysis would help to better generalise the Protection Motivation Theory (PMT) and Digital Resilience Theory (DRT) models in varying institutional settings. Second, longitudinal follow up would be possible in order to monitor the changes in the coping strategies, resilience capacity and technological maturity of SMEs as the digital transformation continues to intensify beyond the post-pandemic period. The long-term observation would help identify whether the adaptive behaviours present in this study are maintained, reduced, or changed in accordance with the new cyber threats and regulatory changes. Third, the next study may be a mixed-methods design that will involve both qualitative interview and quantitative modelling to estimate relationships among perceived severity, coping appraisal and resilience outcomes more accurately. Lastly, the human-organisational interface can be investigated by the author in further work by identifying how leadership attitudes, organisational culture, and employee digital literacy can contribute to SMEs cybersecurity resilience. The following directions would not only make the current study contribute to the existing theoretical field but also enhance the regional policy and practise in sustaining digital sustainability of SME.

6.6.2 Study Limitations

Despite the contributions resulting from this study, the following limitations should be considered when placing findings into context and informing future research:

6.6.2.1 Geographical and sectoral scope

The present study focuses on Abu Dhabi-based SMEs; thus, the general applicability of findings to SMEs in other regions or industries is difficult. Thus, it is likely that the regulatory environment, economic infrastructure, and SME demographics differ between Abu Dhabi and other parts of the UAE or elsewhere. As a result, findings may not depict wholly the ISM challenges and practices of SMEs in other geographical areas or sectors that fall outside the purview of the sample.

6.6.2.2 Qualitative Research Design

The qualitative nature of this study enables a deep exploration of ISM practices and challenges, but it may limit the generalisation of findings to a broader population of SMEs. The results from interviews pertain only to the experiences and views of the respondents, and although they offer rich, contextualized data, they cannot be fully representative of the variances in ISM practices of all SMEs. Results obtained

through mixed-method research with quantitative as well as qualitative data can be more generalisable in varied contexts.

6.6.2.3 Scope of ISM and Digital Adoption Frameworks

The present study embeds Protection Motivation Theory (PMT) as the primary theoretical framework; as such, it provides rich insights into what motivates ISM practices in SMEs. However, this exclusivity may result in the exclusion of other factors that influence these ISM practices, such as organisational and technological readiness or external pressures from the competitive or regulatory environment. Future studies that incorporate additional frameworks could therefore be better placed to capture the overall status of ISM in SMEs.

6.6.2.4 Resources Constraints Affecting Data Collection

Due to resource and logistic limitations in this study, both sample diversity and size remained limited. Access to SMEs depended on the availability and willingness of participants, which can result in the selection bias of overrepresented firms with more proactive approaches to ISM. More ISM experiences could also be captured by increasing the sample size and including SMEs reporting on less mature cybersecurity practices.

6.6.2.5 Dynamic and Evolving Cybersecurity Threat Landscape

Conclusions are based on the findings of cybersecurity challenges during the COVID-19 pandemic, which was a period of unique pressures to rapidly adopt digital technologies for SMEs. As cybersecurity threats change and post-pandemic dynamics stabilize, new challenges and technologies may emerge capable of shifting the ISM landscape for SMEs. This limitation underlines the need for continued research in uncovering emerging threats and technologies in an evolving cybersecurity landscape.

REFERENCES

Aaron, G., Chapin, L., Piscitello, D. and Strutt, C., 2021. Malware landscape 2021. *Interisle Consulting Group, Boston, MA, USA, Tech. Rep. ICGTR-2021-01*.

Abass, I.A.M., 2018. Social engineering threat and defence: a literature survey. *Journal of Information Security*, *9*(04), p.257.

Abbas, W., 2021. Revealed: UAE firms paid more than Dh5.1 million in ransomware, Khaleej Times.

Abdullahi, R. and Mansor, N., 2018. Fraud prevention initiatives in the Nigerian public sector: understanding the relationship of fraud incidences and the elements of fraud triangle theory. *Journal of Financial Crime*.

Abuhussein, T., Barham, H. and Al-Jaghoub, S., 2023. The effects of COVID-19 on small anld medium-sized enterprises: Empirical evidence from Jordan. *Journal of Enterprising Communities: People and Places in the Global Economy, 17*(2), pp.334-357.

ACCA Global, 2016. Cybersecurity in SMEs: People as the weakest link. ACCA Research Report. [online] Available at: https://www.accaglobal.com

ADC, 2019. Small and Medium-sized Enterprises in Abu Dhabi, Abu Dhabi Chamber.

Adeusi, O.C., Adebayo, Y.O., Ayodele, P.A., Onikoyi, T.T., Adebayo, K.B. and Adenekan, I.O., 2024. IT standardization in cloud computing: Security challenges, benefits, and future directions. *World Journal of Advanced Research and Reviews*, *22*(3), pp.2050-2057.

Adu-Gyimah, S., Asante, G. and Boansi, O.K., 2022. Social Engineering Attacks: A Clearer Perspective. *International Journal of Computer Applications*, *975*, p.8887.

Aghghaleh, S.F. and Mohamed, Z.M., 2014. Fraud risk factors of fraud triangle and the likelihood of fraud occurrence: Evidence from Malaysia. *Information Management and Business Review*, *6*(1), pp.1-7.

Ahdadou, H., El Idrissi, N., Boussedra, M., 2022. Digital resilience in SMEs under crisis conditions. International Journal of Business Continuity and Risk Management, 12(4), pp.301-320.

Ahdadou, M., Aajly, A. and Tahrouch, M., 2022. Information Technology Governance: Lessons Learned from The Covid-19 Crisis. *International Journal of Business and Technology Management.*

Ahmed, N. N. and Nanath, K., 2021. Exploring Cybersecurity Ecosystem in the Middle East: Towards an SME Recommender System. *Journal of Cyber Security and Mobility, 10*(3), pp. 511-536.

Ahmed, N.N. and Nanath, K., 2021. Exploring Cybersecurity Ecosystem in the Middle East: Towards an SME Recommender System. *Journal of Cyber Security and Mobility*, pp.511-536.

Ahmed, N.N. and Nanath, K., 2021. Exploring Cybersecurity Ecosystem in the Middle East: Towards an SME Recommender System. *Journal of Cyber Security and Mobility*, pp.511-536.

Akpan, I.J., Udoh, E.A.P. and Adebisi, B., 2022. Small business awareness and adoption of state-of-the-art technologies in emerging and developing markets, and lessons from the COVID-19 pandemic. *Journal of Small Business & Entrepreneurship, 34*(2), pp.123-140.

Al Aina, R. and Atan, T., 2020. The impact of implementing talent management practices on sustainable organizational performance. *Sustainability, 12*(20), p.8372.

Aldawood, H., Skinner, G., 2018. Reviewing cyber security social engineering training and awareness programmes. *Journal of Information Security and Applications*, 40, pp.134-141.

Alferidah, D.K. and Jhanjhi, N.Z., 2020, October. Cybersecurity impact over bigdata and iot growth. In *2020 International Conference on Computational Intelligence (ICCI)* (pp. 103-108). IEEE.

Alhajeri, M., 2022. *Developing a digital competence framework for UAE law enforcement agencies to enhance cyber security of Critical Physical Infrastructure (CPI)*. University of Salford (United Kingdom).

Alharahsheh, H.H. and Pius, A., 2020. A review of key paradigms: Positivism VS interpretivism. *Global Academic Journal of Humanities and Social Sciences*, *2*(3), pp.39-43.

Ali, A., Laghari, A.A., Kandhro, I.A., Kumar, K. and Younus, S., 2024. Systematic analysis of on-premise and cloud services. *International Journal of Cloud Computing*, *13*(3), pp.214-242.

Ali, O., Shrestha, A., Chatfield, A. and Murray, P., 2020. Assessing information security risks in the cloud: A case study of Australian local government authorities. *Government Information Quarterly*, *37*(1), p.101419.

Ali, R., 2021. Looking to the future of the cyber security landscape. *Network Security, 3*, pp. 8-10.

Alketbi, A., Nasir, Q. and Talib, M.A., 2018, February. Blockchain for government services—Use cases, security benefits and challenges. In *2018 15th Learning and Technology Conference (L&T)* (pp. 112-119). IEEE.

Alketbi, A., Nasir, Q. and Talib, M.A., 2018, February. Blockchain for government services—Use cases, security benefits and challenges. In *2018 15th Learning and Technology Conference (L&T)* (pp. 112-119). IEEE.

Alketbi, A.H.S.B., Jimber del Rio, J.A. and Ibáñez Fernández, A., 2022. Exploring the role of human resource development functions on crisis management: The case of Dubai-UAE during Covid-19 crisis. *PloS one*, *17*(3), p.e0263034.

Al-Monitor, 2020. Cyberattacks in UAE up 250% during the pandemic, Emirati cyber chief says. [Online]

Alnajjar, M.I.M., 2017. Impact of accounting information system on organizational performance: A study of SMEs in the UAE. *Global Review of Accounting and Finance*, *8*(2), pp.20-38.

Alnajjar, M.I.M., 2017. Impact of accounting information system on organizational performance: A study of SMEs in the UAE. *Global Review of Accounting and Finance*, *8*(2), pp.20-38.

Alomari, E., Manickam, S., Gupta, B.B., Karuppayah, S. and Alfaris, R., 2012. Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art. *arXiv preprint arXiv:1208.0403*.

Alsharari, N.M., Al-Shboul, M. and Alteneiji, S., 2020. Implementation of cloud ERP in the SME: evidence from UAE. *Journal of Small Business and Enterprise Development*.

Al-Sharji, A., Ahmad, S. Z. and Bakar, A. R. A., 2021. Understanding social media adoption in SMEs: Empirical evidence from the United Arab Emirates. *Journal of Entrepreneurship in Emerging Economies, 10*(10).

Alshehhi, K.M., 2017. *The Preparedness of SMEs for cyber risk in the United Arab Emirates* (Doctoral dissertation, The British University in Dubai (BUiD)).

Altaher, N., 2016. UAE a target of 5 per cent of global cyber-attacks. [Online]

Alzahrani, A., Alshehri, A., Alshahrani, H. and Fu, H., 2020. Ransomware in Windows and Android platforms. *arXiv preprint arXiv:2005.05571*.

Anderson, A., Ahmad, A. and Chang, S., 2024. Case-Based Learning for Cybersecurity Leaders: A Systematic Review and Research Agenda. *Information & Management*, p.104015.

Anderson, R., Ahmad, A. Chang, E., 2024. Cyber resilience of SMEs in the post-pandemic digital economy. *Journal of Cybersecurity and Digital Trust*, *12*(2), pp.45-62.

Antwi, S.K. and Hamza, K., 2015. Qualitative and quantitative research paradigms in business research: A philosophical reflection. *European journal of business and management*, *7*(3), pp.217-225.

Apriani, A., Wahdiniawati, S.A., Perkasa, D.H., Magita, M., Meliantari, D. and Widayati, C., 2024. Digital Transformation of SMEs: Boosting Online Shopping Interest through E-Commerce Adoption. *Dinasti International Journal of Digital Business Management*, *5*(3), pp.595-611.

Armenia, S., Angelini, M., Nonino, F., Palombi, G. and Schlitzer, M.F., 2021. A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, *147*, p.113580.

Arroyabe, I. F. D. and Arroyabe, J. C. F. D., 2021. The severity and effects of Cyber-breaches in SMEs: a machine learning approach. *Enterprise Information Systems*, pp. 1-27.

Arroyabe, M.F., Arranz, C.F., de Arroyabe, I.F. and de Arroyabe, J.C.F., 2024. The effect of IT security issues on the implementation of industry 4.0 in SMEs: Barriers and challenges. *Technological Forecasting and Social Change*, *199*, p.123051.

Asgari, S., Trajkovic, J., Rahmani, M., Zhang, W., Lo, R.C. and Sciortino, A., 2021. An observational study of engineering online education during the COVID-19 pandemic. *Plos one*, *16*(4), p.e0250041.

Asnawi, A., Riyani, R., Akob, B. and Hanafiah, H., 2020. *Historical Gossip as Social Engineering to Build Historical Awareness*. Available at: https://eprints.eudl.eu/id/eprint/2671/1/eai.20-6-2020.2300711.pdf [accessed 6 June 2022]

Asnawi, A.L., Yusof, R., Ahmad, R., 2020. Profiling social engineering attack strategies. *Journal of Information Assurance and Cybersecurity*, 2020, pp.1-12.

Astakhova, L.V. and Medvedev, I.A., 2021. An information tool for increasing the resistance of employees of an organization to social engineering attacks. *Scientific and Technical Information Processing*, *48*(1), pp.15-20.

Atoum, I., Otoom, A. and Ali, A.A., 2014. A holistic cyber security implementation framework. *Information Management & Computer Security*.

Azhar, M.B.M., Azlan, W.N.A.W.A., Mazri, W.N.A.W. and Radzi, S.M., 2023. Social Engineering and Cyber Threats: Exploring Techniques, Impacts and Strategies. *International Journal of Accounting, Finance and Business*, *8*(50).

Azizi, N. and Haass, O., 2023. Cybersecurity issues and challenges. In *Handbook of research on Cybersecurity issues and challenges for business and FinTech applications* (pp. 21-48). IGI Global.

Bai, C., Quayson, M. and Sarkis, J., 2021. COVID-19 pandemic digitization lessons for sustainable development of micro-and small-enterprises. *Sustainable Production and Consumption, 27*, pp.1989-2001.

Baig, A., Hall, B., Jenkins, P., Lamarre, E. and McCarthy, B., 2020. The COVID-19 recovery will be digital: A plan for the first 90 days. *McKinsey Digital*, *14*.

Bairagi, V. and Munot, M.V. eds., 2019. *Research methodology: A practical and scientific approach*. CRC Press.

Babbie, E. R. (2013). *The basics of social research*. Cengage Learning.

Bakdash, J.Z., Hutchinson, S., Zaroukian, E.G., Marusich, L.R., Thirumuruganathan, S., Sample, C., Hoffman, B. and Das, G., 2018. Malware in the future? Forecasting of analyst detection of cyber events. *Journal of Cybersecurity*, *4*(1), p.tyy007.

Balarezo, J.F., Wang, S., Chavez, K.G., Al-Hourani, A. and Kandeepan, S., 2021. A survey on DoS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks. *Engineering Science and Technology, an International Journal*.

Bandari, V., 2023. Enterprise data security measures: a comparative review of effectiveness and risks across different industries and organization types. *International Journal of Business Intelligence and Big Data Analytics*, *6*(1), pp.1-11.

Banister, P., Bunn, G., Burman, E., Daniels, J., Duckett, P., Goodley, D., Lawthom, R., Parker, I., Runswick-Cole, K., Sixsmith, J. and Smailes, S., 2011. *EBOOK: Qualitative Methods in Psychology: A Research Guide*. McGraw-Hill Education (UK).

Barker, A., Varghese, B., Ward, J.S. and Sommerville, I., 2014. Academic cloud computing research: Five pitfalls and five opportunities. In *6th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 14)*.

Barnum, S., 2012. Standardizing cyber threat intelligence information with the structured threat information expression (stix). *Mitre Corporation*, *11*, pp.1-22.

Başer, M., Güven, E.Y. and Aydın, M.A., 2021, September. SSH and Telnet Protocols Attack Analysis Using Honeypot Technique:* Analysis of SSH AND TELNET Honeypot. In *2021 6th International Conference on Computer Science and Engineering (UBMK)* (pp. 806-811). IEEE.

Behal, S. and Kumar, K., 2017. Detection of DDoS attacks and flash events using novel information theory metrics. *Computer Networks*, *116*, pp.96-110.

Ben-Asher, N. and Gonzalez, C., 2015. Effects of cyber security knowledge on attack detection. *Computers in Human Behaviour*, *48*, pp.51-61.

Bingham, A.J. and Witkowsky, P., 2021. Deductive and inductive approaches to qualitative data analysis. *Analyzing and interpreting qualitative data: After the interview*, *1*, pp.133-146.

Black, P. and Opacki, J., 2016, October. Anti-analysis trends in banking malware. In *2016 11th International Conference on Malicious and Unwanted Software (MALWARE)* (pp. 1-7). IEEE.

Blackwood-Brown, C., Levy, Y. and D'Arcy, J., 2021. Cybersecurity awareness and skills of senior citizens: a motivation perspective. *Journal of Computer Information Systems*, *61*(3), pp.195-206.

Blackwood-Brown, C.G., 2018. *An Empirical Assessment of Senior Citizens' Cybersecurity Awareness, Computer Self-Efficacy, Perceived Risk of Identity Theft, Attitude, and Motivation to Acquire Cybersecurity Skills* (Doctoral dissertation, Nova Southeastern University).

Blakley, B., McDermott, E. and Geer, D., 2001, September. Information security is information risk management. In *Proceedings of the 2001 workshop on new security paradigms* (pp. 97-104).

Bless, C., Higson-Smith, C. and Kagee, A., 2006. *Fundamentals of social research methods: An African perspective*. USA: Juta and Company Ltd.

Boehm, J., Curcio, N., Merrath, P., Shenton, L. and Stähle, T., 2019. The risk-based approach to Cybersecurity. *McKinsey, New York*.

Bouyer, A. and Arasteh, B., 2014. The necessity of using cloud computing in educational system. *Procedia-Social and Behavioural Sciences*, *143*, pp.581-585.

Braun, V. and Clarke, V., 2012. *Thematic analysis*. American Psychological Association. https://psycnet.apa.org/doi/10.1037/13620-004

Braun, V. and Clarke, V., 2012. Thematic analysis. *American Psychological Association.* https://psycnet.apa.org/doi/10.1037/13620-004

Braun, V. and Clarke, V., 2021. Thematic analysis: A practical guide.

Bresler, L. and Stake, R.E., 2017. Qualitative research methodology in music education. *Critical essays in music education*, pp.113-128.

Broadhurst, R. and Trivedi, H., 2020. Malware in spam email: Risks and trends in the Australian Spam Intelligence Database. *Trends and Issues in Crime and Criminal Justice [electronic resource]*, (603), pp.1-18.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., Filar, B. and Anderson, H., 2018. The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint arXiv:1802.07228*.

Buckley, P.J., 2016. Historical research approaches to the analysis of internationalisation. *Management International Review*, *56*(6), pp.879-900.

Burda, P., Allodi, L. and Zannone, N., 2024. Cognition in social engineering empirical research: a systematic literature review. *ACM Transactions on Computer-Human Interaction*, *31*(2), pp.1-55.

Burrell, D.N., Nobles, C., Cusak, A., Jones, L.A., Wright, J.B., Mingo, H.C., Ferreras-Perez, J., Khanta, K., Shen, P. and Richardson, K., 2023. Cybersecurity and Cyberbiosecurity Insider Threat Risk Management. In *Handbook of Research on Cybersecurity Risk in Contemporary Business Systems* (pp. 121-136). IGI Global.

Carstens, D.S., McCauley-Bell, P.R., Malone, L.C. and DeMara, R.F., 2004. Evaluation of the human impact of password authentication practices on information security.

Chaudhary, S., Gkioulos, V. and Katsikas, S., 2023. A quest for research and knowledge gaps in Cybersecurity awareness for small and medium-sized enterprises. *Computer Science Review*, *50*, p.100592.

Check Point Software Technologies, 2019. *Cyber security report 2019: Threat intelligence trends.* [online] Check Point. Available at: https://www.checkpoint.com/downloads/resources/cyber-security-report-2019.pdf [Accessed 21 Mar. 2025].

Chen, H. and Hai, Y., 2024. Exploring the critical success factors of information security management: a mixed-method approach. *Information & Computer Security*.

Chen, Q. and Bridges, R.A., 2017, December. Automated behavioural analysis of malware: A case study of wannacry ransomware. In *2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA)* (pp. 454-460). IEEE.

Cheung, K.F., Bell, M.G. and Bhattacharjya, J., 2021. Cybersecurity in logistics and supply chain management: An overview and future research directions. Transportation Research Part E: *Logistics and Transportation Review, 146*, p.102217.

Chidukwani, A., Zander, S. and Koutsakis, P., 2022. A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations. *IEEE Access*, *10*, pp.85701-85719.

Chitrey, A., Singh, D. and Singh, V., 2012. A comprehensive study of social engineering based attacks in India to develop a conceptual model. *International Journal of Information and Network Security*, *1*(2), p.45.

Chitrey, A., Singh, G., Singh, P., 2012. Social engineering: A partial technical attack. International Conference on Advances in Computing and Communications, pp.76-82.

Clarke, N. and Furnell, S. eds., 2020. *Human Aspects of Information Security and Assurance: 14th IFIP WG 11.12 International Symposium, HAISA 2020, Mytilene, Lesbos, Greece, July 8–10, 2020, Proceedings* (Vol. 593). UK: Springer Nature.

CNBC, 2021. Meat supplier JBS paid ransomware hackers $11 million/ https://www.cnbc.com/2021/06/09/jbs-paid-11-million-in-response-to-ransomware-attack-.html#:~:text=Signage%20outside%20the%20JBS%20Beef,Tuesday%2C%20June%201%2C%202021.&text=JBS%2C%20the%20largest%20beef%20supplier,million%2C%20the%20company%20said%20Wednesday.

Conteh, N.Y., 2021. The dynamics of social engineering and cybercrime in the digital age. In *Ethical Hacking Techniques and Countermeasures for Cybercrime Prevention* (pp. 144-149). IGI Global.

Costa, J. and Castro, R., 2021. SMEs must go online—E-commerce as an escape hatch for resilience and survivability. *Journal of Theoretical and Applied Electronic Commerce Research, 16*(7), pp.3043-3062.

Costa, J. and Castro, R., 2021. SMEs Must Go Online—E-Commerce as an Escape Hatch for Resilience and Survivability. *Journal of Theoretical and Applied Electronic Commerce Research, Volume 16*, pp. 3043-3062.

Couce-Vierira, A., Insua, D. R. and Kosgodagan, A., 2020. Assessing and Forecasting Cybersecurity Impacts. *Decision Analysis, 17*(4), pp. 356-374.

Cr, K., 2020. Research methodology methods and techniques.

Craciun, V.C., Mogage, A. and Simion, E., 2018, November. Trends in design of ransomware viruses. In *International Conference on Security for Information Technology and Communications* (pp. 259-272). Springer, Cham.

Creswell, J.W. and Creswell, J.D., 2017. *Research design: Qualitative, quantitative, and mixed methods approaches*. UK: Sage publications.

Cusmano, L. and Raes, S., 2020. OECD Policy Responses to Coronavirus (COVID-19); Coronavirus (COVID-19): SME policy responses. *Retrieved from OECD Better Policies for Better Lives: http://www. OECD. Org/coronavirus/policy-responses/coronavirus-covid-19-sme-policy-responses-04440101/# section-d1e160*.

Cybereason, 2021. Ransomware: The True Cost To Business: Cybereason.

De Kimpe, L., Walrave, M., Verdegem, P. and Ponnet, K., 2022. What we think we know about Cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour & Information Technology*, *41*(8), pp.1796-1808.

de Oliveira, A. and Sassi, R.J., 2020. Chimera: an android malware detection method based on multimodal deep learning and hybrid analysis. *TechRxiv*.

Dong, S., Abbas, K. and Jain, R., 2019. A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments. *IEEE Access*, *7*, pp.80813-80828.

Douligeris, C. and Mitrokotsa, A., 2004. DDoS attacks and defence mechanisms: classification and state-of-the-art. *Computer networks*, *44*(5), pp.643-666.

Duan, Q. and Al-Shaer, E., 2013. Traffic-aware dynamic firewall policy management: techniques and applications. *IEEE Communications Magazine*, *51*(7), pp.73-79.

Dwivedi, Y.K., Hughes, D.L., Coombs, C., Constantiou, I., Duan, Y., Edwards, J.S., Gupta, B., Lal, B., Misra, S., Prashant, P. and Raman, R., 2020. Impact of COVID-19 pandemic on information management research and practice: Transforming education, work and life. *International journal of information management, 55*, p.102211.

Easterby-Smith, M., Jaspersen, L.J., Thorpe, R. and Valizade, D., 2021. *Management and business research*. Sage.

Egami, N. and Hartman, E., 2023. Elements of external validity: Framework, design, and analysis. *American Political Science Review*, *117*(3), pp.1070-1088.

Elbeltagi, I., Al Sharji, Y., Hardaker, G. and Elsetouhi, A., 2013. The role of the owner-manager in SMEs' adoption of information and communication technology in the United Arab Emirates. *Journal of Global Information Management (JGIM)*, *21*(2), pp.23-50.

enhancing SMEs' resilience in the context of COVID-19. *Sustainability, 13*(12), p.6542.

ESET Security, 2018. ESET Threat Report: GandCrab and ransomware evolution. *ESET Security Research*, pp.1-32.

European Data Protection Supervisor, 2020. *A Preliminary Opinion on data protection and scientific research*. Available at: https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf [accessed on 22nd November 2023]

Farouk, H., 2017. Cyber-crime: avoid paying the price protecting your business, Grant Thornton.

Fawcett, T., 2020. Human error as a cybersecurity vulnerability. *Information Security Journal*, *29*(3), pp.123-132.

Fayomi, O., Ndubisi, O.N., Ayo, C., Chidozie, F., Ajayi, L. and Okorie, U., 2015, June. Cyber-attack as a menace to effective governance in Nigeria. In *Proceedings of the 15th European Conference on eGovernment ECEG 2015 University of Portsmouth* (p. 107).

FireEye, 2016. 5 Reasons Cyber Attackers Target SMEs, FireEye.

Floyd, D.L., Prentice-Dunn, S. and Rogers, R.W., 2000. A meta-analysis of research on protection motivation theory. *Journal of applied social psychology*, *30*(2), pp.407-429.

Forbes, 2022. Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know. https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=64ca4dce7864

Franco, M.F., Lacerda, F.M. and Stiller, B., 2022. A framework for the planning and management of Cybersecurity projects in small and medium-sized enterprises. *Revista de Gestão e Projetos*, *13*(3), pp.10-37.

Gabriel, Y., 2015. Reflexivity and beyond–a plea for imagination in qualitative research methodology. *Qualitative Research in Organizations and Management: An International Journal*.

Galeano-Brajones, J., Carmona-Murillo, J., Valenzuela-Valdés, J.F. and Luna-Valero, F., 2020. Detection and mitigation of dos and DDoS attacks in IoT-based stateful sdn: An experimental approach. *Sensors*, *20*(3), p.816.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q. and Laplante, P., 2011. Dimensions of cyber-attacks: Cultural, social, economic, and political. *IEEE Technology and Society Magazine*, *30*(1), pp.28-38.

Gattis, V.M., 2018. *Bullied! Coping with workplace bullying*. Dissertation.com.

Gazet, A., 2010. Comparative analysis of various ransomware virii. *Journal in computer virology*, *6*(1), pp.77-90.

Gezer, A., Warner, G., Wilson, C. and Shrestha, P., 2019. A flow-based approach for Trickbot banking trojan detection. *Computers & Security*, *84*, pp.179-192.

Giuffrida, C., Bardin, S. and Blanc, G. eds., 2018. *Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 92-111). UK: Springer International Publishing.

Glesne, C., 2016. *Becoming qualitative researchers: An introduction*. Pearson. One Lake Street, Upper Saddle River, New Jersey 07458.

Golinelli, D., Boetto, E., Carullo, G., Nuzzolese, A.G., Landini, M.P. and Fantini, M.P., 2020. Adoption of digital technologies in health care during the COVID-19 pandemic: systematic review of early scientific literature. *Journal of medical Internet research*, *22*(11), p.e22280.

Goodwin, C.F. and Nicholas, J.P., 2013. Developing a National strategy for Cyber Security. *Foundation for Security Growth and Innovation*.

Goyal, S., 2014. Public vs private vs hybrid vs community-cloud computing: a critical review. *International Journal of Computer Network and Information Security*, *6*(3), pp.20-29.

Grassegger, T. and Nedbal, D., 2021. The role of employees' information security awareness on the intention to resist social engineering. *Procedia Computer Science*, *181*, pp.59-66.

Greitzer, F.L. and Frincke, D.A., 2010. Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation. In *Insider threats in cyber security* (pp. 85-113). Springer, Boston, MA.

Gressin, S., 2017. The equifax data breach: What to do. *Federal Trade Commission*, *8*.

Groenewold, W.G.F. and Lessard-Phillips, L., 2012. Research methodology. *The European second generation compared: does the integration context matter?*

Guarnizo, J.D., Tambe, A., Bhunia, S.S., Ochoa, M., Tippenhauer, N.O., Shabtai, A. and Elovici, Y., 2017, April. Siphon: Towards scalable high-interaction physical honeypots. In *Proceedings of the 3rd ACM Workshop on Cyber-Physical System Security* (pp. 57-68).

Gunasekare, U.L.T.P., 2015. Mixed research method as the third research paradigm: a literature review. *University of Kelaniya*.

Hadnagy, C., 2010. *Social engineering: The art of human hacking*. John Wiley & Sons.

Hakmeh, J., 2017. *Cybercrime and the Digital Economy in the GCC Countries*. London: Chatham House.

Hamamreh, J.M., Furqan, H.M. and Arslan, H., 2018. Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, *21*(2), pp.1773-1828.

Hassib, B. and Shires, J., 2022. Cybersecurity in the GCC: From Economic Development to Geopolitical Controversy. Middle East Policy/ Early View, pp. 1-1.

Hau, B., Penrose, M., Hall, T. and Bevilacqua, M., 2016. M-Trends 2016 EMEA Edition, Mandiant.

He, C.Z., Frost, T. and Pinsker, R.E., 2020. The impact of reported Cybersecurity breaches on firm innovation. *Journal of Information Systems, 34*(2), pp.187-209.

Help AG/Etisalat, 2021. Cybersecurity Everywhere: State of the Market Report, Help AG.

Hijji, M. and Alam, G., 2021. A multivocal literature review on growing social engineering based cyber-attacks/threats during the COVID-19 pandemic: challenges and prospective solutions. *Ieee Access*, *9*, pp.7152-7169.

Hodge, C., Hauck, K., Gupta, S. and Bennett, J.C., 2019. *Vehicle Cybersecurity threats and mitigation approaches* (No. NREL/TP-5400-74247). National Renewable Energy Lab.(NREL), Golden, CO (United States).

Hoffmann, R., Napiórkowski, J., Protasowicki, T. and Stanik, J., 2020. Risk based approach in scope of Cybersecurity threats and requirements. *Procedia Manufacturing*, *44*, pp.655-662.

Hollnagel, E., 2017. *Safety-II in practice: developing the resilience potentials*. Routledge. *ISO/IEC 27001:2020 Information Security Management Systems — Requirements.* Geneva: International Organization for Standardization.

Homer, E.M., 2020. Testing the fraud triangle: a systematic review. *Journal of Financial Crime*.

Hoque, N., Bhattacharyya, D.K. and Kalita, J.K., 2015. Botnet in DDoS attacks: trends and challenges. *IEEE Communications Surveys & Tutorials*, *17*(4), pp.2242-2270.

Howitt, D., 2019. *Introduction to qualitative research methods in psychology*. pearson UK.

Huber, W., 2017. Forensic accounting, fraud theory, and the end of the fraud triangle. *Journal of Theoretical Accounting Research*, *12*(2).

Hughes, L.A. and DeLone, G.J., 2007. Viruses, worms, and Trojan horses: Serious crimes, nuisance, or both?. *Social science computer review*, *25*(1), pp.78-98.

Humphreys, E., 2008. Information security management standards: Compliance, governance and risk management. *Information security technical report*, *13*(4), pp.247-255.

Huseynov, F. and Ozdenizci Kose, B., 2024. Using machine learning algorithms to predict individuals' tendency to be victim of social engineering attacks. *Information Development*, *40*(2), pp.298-318.

Hussain, I., 2021. Cyberattacks on UAE small businesses up 183% in 2020 – report, Gulf Business.

Huxley, 2020. *An overview of the Cyber Security landscape in the UAE*. [Online] Huxley. Available at: <https://www.huxley.com/en-gb/blog/2019/06/an-overview-of-the-cyber-security-landscape-in-the-uae/> [Accessed 17 August 2022].

Huyghue, B.D., 2021. Cybersecurity, Internet of Things, and Risk Management for Businesses (Doctoral dissertation, Utica College).

IBP Inc., 2013. *EU Cyber Security Strategy and Programs Handbook Volume 1 Strategic Information and Regulations*. Australia: Lulu.com

Idir, A. A. B., Karim, S. and El-Najjar, N., 2021. Cybersecurity: Trends and developments in the UAE. In: *R. A. C. and S. Austin, eds. Cybersecurity. s.l.: Chambers and Partners*, pp. 191-194.

Ikmal, A. et al., 2020. Small and Medium Enterprises in the Pandemic: Impact, Responses and the Role of Development Finance. In: *Policy Research Working Papers. Washington*: World Bank Group.

Indriastuti, M. and Fuad, K., 2021. Impact of covid-19 on digital transformation and sustainability in small and medium enterprises (smes): A conceptual framework. In *Complex, Intelligent and Software Intensive Systems: Proceedings of the 14th International Conference on Complex, Intelligent and Software Intensive Systems (CISIS-2020)* (pp. 471-476). Springer International Publishing.

Interpol, 2020. Cybercrime: COVID Impact, Interpol.

Isachenko, N. N., 2018. The Role of Information and Informational and Communication Technologies in Modern Society. *Utopía y Praxis Latinoamericana, 23*(82), pp. 361-67.

Islam, M.M., Dutta, A., Sajid, M.S.I., Al-Shaer, E., Wei, J. and Farhang, S., 2021, October. CHIMERA: Autonomous Planning and Orchestration for Malware Deception. In *2021 IEEE Conference on Communications and Network Security (CNS)* (pp. 173-181). IEEE.

Ivaldi, S., Scaratti, G. and Fregnan, E., 2022. Dwelling within the fourth industrial revolution: organizational learning for new competences, processes and work cultures. *Journal of Workplace Learning*, *34*(1), pp.1-26.

Jahankhani, H., Carlile, A., Emm, D., Hosseinian-Far, A., Brown, G., Sexton, G. and Jamal, A., 2017, May. Global Security, Safety and Sustainability-The Security Challenges of the Connected World. In *ICGS3: International Conference on Global Security, Safety, and Sustainability*. UK: Springer.

Jain, P., 2024. Cloud Adoption Strategies for Small and Medium Enterprises (SMEs): A Comprehensive Guide to Overcoming Challenges and Maximizing Benefits. *Sch J Eng Tech*, *1*(1), pp.28-30.

Jamil, H., Zia, T., Nayeem, T., Whitty, M.T. and D'Alessandro, S., 2024. Human-centric cyber security: Applying protection motivation theory to analyse micro business owners' security behaviours. *Information & Computer Security*.

Jamil, H., Zia, T., Nayeem, T., Whitty, M.T. and D'Alessandro, S., 2024. Human-centric cyber security: Applying protection motivation theory to analyse micro business owners' security behaviours. *Information & Computer Security*.

Jamshed, S., 2014. Qualitative research method-interviewing and observation. *Journal of basic and clinical pharmacy*, *5*(4), p.87.

Jasper, R., 2015. Cybercrime and the rising role of malicious agents. *Cyber Defense Review*, *3*(1), pp.14-25.

Jawandhiya, P.M., Ghonge, D., Ali, M.S. and Deshpande, J.S., 2010. A survey of mobile ad hoc network attacks. *International Journal of Engineering Science and Technology*, *2*(9), pp.4063-4071.

Jayarao, G.B., Ray, S. and Panigrahi, P.K., 2024. Information security threats and organizational readiness in nWFH scenarios. *Computers & Security*, *140*, p.103745.

Johnson, R.B. and Christensen, L., 2019. *Educational research: Quantitative, qualitative, and mixed approaches*. UK: Sage publications.

Junger, M., Montoya, L. and Overink, F.J., 2017. Priming and warnings are not effective to prevent social engineering attacks. *Computers in human behaviour*, *66*, pp.75-87.

Junger, M., Montoya, L., Overink, F., 2017. Priming and social engineering: The role of authority and trust. *Crime Science*, *6*(8), pp.1-9.

Kaloudi, N. and Li, J., 2020. The ai-based cyber threat landscape: A survey. *ACM Computing Surveys (CSUR)*, *53*(1), pp.1-34.

Kamal, S.S.L.B.A., 2019. Research paradigm and the philosophical foundations of a qualitative study. *PEOPLE: International Journal of Social Sciences*, *4*(3), pp.1386-1394.

Karpasitis, C. ed., 2020, July. *ECSM 2020 8th European conference on social media*. USA: Academic Conferences and publishing limited.

Kaspersky Lab, 2015. IT Threat Evolution Report 2015. Kaspersky Security Bulletin, pp.1-45.

Kassem, R. and Higson, A., 2012. The new fraud triangle model. *Journal of emerging trends in economics and management sciences*, *3*(3), pp.191-195.

Kaur, S.J., Ali, L., Hassan, M.K. and Al-Emran, M., 2021. Adoption of digital banking channels in an emerging economy: exploring the role of in-branch efforts. *Journal of Financial Services Marketing*, *26*, pp.107-121.
Kaur, S.J., Ali, L., Hassan, M.K. and Al-Emran, M., 2021. Adoption of digital banking channels in an emerging economy: exploring the role of in-branch efforts. *Journal of Financial Services Marketing*, *26*, pp.107-121.
Kaushik, V. and Walsh, C.A., 2019. Pragmatism as a research paradigm and its implications for social work research. *Social sciences*, *8*(9), p.255.

Khaldi, K., 2017. Quantitative, qualitative or mixed research: which research paradigm to use?. *Journal of Educational and Social Research*, *7*(2), pp.15-15.

Kishore, B, K., 2023. *Intelligent Engineering Applications and Applied Sciences for Sustainability*. Germany: IGI Global

Klein, V.B. and Todesco, J.L., 2021. COVID-19 crisis and SMEs responses: The role of digital transformation. *Knowledge and Process Management*, *28*(2), pp.117-133.

Klimburg-Witjes, N. and Wentland, A., 2021. Hacking humans? Social Engineering and the construction of the "deficient user" in Cybersecurity discourses. *Science, Technology, & Human Values*, *46*(6), pp.1316-1339.

Ključnikov, A., Mura, L. and Sklenár, D., 2019. Information security management in SMEs: factors of success. *Entrepreneurship and Sustainability Issues, 6*(4), p.2081.

Kolias, C., Kambourakis, G., Stavrou, A. and Voas, J., 2017. DDoS in the IoT: Mirai and other botnets. *Computer*, *50*(7), pp.80-84.

Korba, A.A., Nafaa, M. and Salim, G., 2013, April. Survey of routing attacks and countermeasures in mobile ad hoc networks. In *2013 UKSim 15th International Conference on Computer Modelling and Simulation* (pp. 693-698). IEEE.

Kovalainen, A. and Eriksson, P., 2015. Qualitative methods in business research: A practical guide to social research. *Qualitative Methods in Business Research*, pp.1-376.

Kraemer, S. and Carayon, P., 2007. Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. *Applied ergonomics*, *38*(2), pp.143-154.

Krombholz, K., Hobel, H., Huber, M. and Weippl, E., 2015. Advanced social engineering attacks. *Journal of Information Security and applications*, *22*, pp.113-122.

Krombholz, K., Hobel, H., Huber, M., Weippl, E., 2015. Social engineering attacks: A survey. *Journal of Information Security and Applications*, 22, pp.18-31.

Kshetri, N., 2013. Cybercrime and cyber-security issues associated with China: some economic and institutional considerations. *Electronic Commerce Research*, *13*(1), pp.41-69.

Kuada, J., 2012. *Research methodology: A project guide for university students*. Samfundslitteratur.

Kumar, M. and Ayedee, D., 2021. Technology Adoption: A Solution for SMEs to overcome problems during COVID-19. *Forthcoming, Academy of Marketing Studies Journal, 25*(1).

Kumar, R., 2018. *Research methodology: A step-by-step guide for beginners*. Sage.

Kumar, R., Rajesh, S., Awasthi, R., 2015. Corporate vulnerabilities to social engineering. *International Journal of Computer Security*, *9*(3), pp.55-67.

Kumar, S. and Carley, K.M., 2016, September. Approaches to understanding the motivations behind cyber-attacks. In *2016 IEEE Conference on Intelligence and Security Informatics (ISI)* (pp. 307-309). IEEE.

Kunduru, A.R., 2023. The perils and defences of enterprise cloud computing: a comprehensive review. *Central Asian Journal of Mathematical Theory and Computer Sciences*, *4*(9), pp.29-41.

Kuzmenko, O.V., 2020. Trends of fraud operations on the banking market and approaches of Cybersecurity assessment.

Lacey, D., Salmon, P. and Glancy, P., 2015. Taking the bait: a systems analysis of phishing attacks. *Procedia Manufacturing*, *3*, pp.1109-1116.

Lallie, H.S., Shepherd, L.A., Nurse, J.R., Erola, A., Epiphaniou, G., Maple, C. and Bellekens, X., 2021. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & security*, *105*, p.102248.

Lanz, J. and Sussman, B.I., 2020. Information security program management in a COVID-19 world. *The CPA Journal*, *90*(6), pp.28-35.

Lanz, J. and Sussman, B.I., 2020. Information Security Program Management in a COVID-19 World. *CPA Journal*, *90*(6).

Lee, K., Kim, J., Kwon, K.H., Han, Y. and Kim, S., 2008. DDoS attack detection method using cluster analysis. *Expert systems with applications*, *34*(3), pp.1659-1665.

Lee, S.Z., 2020. A basic principle of physical security and its link to Cybersecurity. *International Journal of Cyber Criminology*, *14*(1), pp.203-219.

Lee, V. and Herstatt, C., 2015. How Firms Can Strategically Influence Open Source Communities: The Employment of ‘Men on the Inside'. In *Open Source Innovation* (pp. 229-263). USA: Routledge.

LeFebvre, R., 2012, October. The human element in cyber security: a study on student motivation to act. In *Proceedings of the 2012 Information Security Curriculum Development Conference* (pp. 1-8).

Lemmou, A., Souidi, S., 2018. Analysis of GandCrab ransomware attacks. *Journal of Information Security Research*, *9*(2), pp.37-48.

Lemmou, Y. and Souidi, E.M., 2018, September. Inside gandcrab ransomware. In *International Conference on Cryptology and Network Security* (pp. 154-174). Springer, Cham.

Li, W., Jin, J. and Lee, J.-K., 2019. Analysis of Botnet Domain Names for IoT Cybersecurity. IEEE Access, 7(2019), pp. 94658-94664.

Lin, X., Wang, X. and Hajli, N., 2019. Building E-Commerce Satisfaction and Boosting Sales: The Role of Social Commerce Trust and Its Antecedents. Int. J. Electron. Commer. 23, pp. 328-363.

Lu, Y. and Wang, M., 2016, June. An easy defence mechanism against botnet-based DDoS flooding attack originated in SDN environment using sFlow. In *Proceedings of the 11th International Conference on Future Internet Technologies* (pp. 14-20).

Luo X, Brody R, Seazzu A, Burd S. 2011. Social engineering: the neglected human factor for information security management. *Information Resources Management Journal, 24*(3), pp. 1-8.

Mack, L., 2010. The philosophical underpinnings of educational research.

Maher, A., 2022. UAE shores up cyber defences to thwart hackers, The National News.

Malecki, F., 2020. Overcoming the Security Risks of Remote Working. *Computer Fraud and Security, 7*(2020), pp. 10-12.

Mansor, N. and Abdullahi, R., 2015. Fraud triangle theory and fraud diamond theory. Understanding the convergent and divergent for future research. *International Journal of Academic Research in Accounting, Finance and Management Science*, *1*(4), pp.38-45.

Mansor, N., 2015. Concomitant debacle of fraud incidences in the Nigeria public sector: Understanding the power of fraud triangle theory. *International journal of academic research in business and social sciences*, *5*(9), pp.2222-6990.

Mantha, B.R. and de Soto, B.G., 2019. Cyber security challenges and vulnerability assessment in the construction industry. In *Creative Construction Conference 2019* (pp. 29-37). Budapest University of Technology and Economics.

Manurung, D.T. and Hadian, N., 2013, November. Detection fraud of financial statement with fraud triangle. In *Proceedings of 23rd International Business Research Conference* (Vol. 36, No. 8, pp. 1-18).

Manzoor, J., Waleed, A., Jamali, A.F. and Masood, A., 2024. Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs. *Plos one*, *19*(3), p.e0301183.

Marhad, S.S., Abd Goni, S.Z. and Sani, M.K.J.A., 2024. Implementation of Information Security Management Systems for Data Protection in Organizations: A systematic literature review. *Environment-Behaviour Proceedings Journal*, *9*(SI18), pp.197-203.

Maslan, A., Mohammad, K.M. and Arnomo, S.A., 2018, November. DDoS detection on network protocol using cosine similarity and N-Gram+ Method. In *2018 International Conference on Sustainable Information Engineering and Technology (SIET)* (pp. 234-239). IEEE.

Matsumoto, S., Hitz, S. and Perrig, A., 2014, August. Fleet: Defending SDNs from malicious administrators. In *Proceedings of the third workshop on hot topics in software defined networking* (pp. 103-108).

Mazdar, D., 2018. Contribution of Knowledge Management to the Development of Enterprises. University of Rijeka, ToSEE.

Mc Manus, P., Mulhall, S., Ragab, M. and Arisha, A., 2017, June. An investigation in the methodological approaches used in doctoral business research in Ireland. In *ECRM 2017 16th European Conference on Research Methods in Business and Management* (p. 233). Academic Conferences and publishing limited.

Medan, I., 2020, June. The Effect of the Role of The Internal Control System on Good University Governance In Private Education. In *ICASI 2020: Proceedings of the 3rd International Conference on Advance & Scientific Innovation, ICASI 2020, 20 June 2020, Medan, Indonesia* (p. 120). European Alliance for Innovation.

Medan, N., 2020. Psychology of social engineering in modern cybercrime. *Cybersecurity and Ethics Journal*, *5*(2), pp.101-118.

Meland, P.H., Nesheim, D.A., Bernsmed, K. and Sindre, G., 2022. Assessing cyber threats for storyless systems. *Journal of Information Security and Applications*, *64*, p.103050.

Merritt, J., 2021. COVID -19 and Technology Adoption in Small and Medium-Sized Enterprises: The Impact and the Way Forward, *World Economic Forum.*

Mertens, D.M., 2012. What comes first? The paradigm or the approach? *Journal of mixed methods research*, *6*(4), pp.255-257.

Meyers, C.A., Powers, S.S. and Faissol, D.M., 2009. *Taxonomies of cyber adversaries and attacks: a survey of incidents and approaches* (No. LLNL-TR-419041). Lawrence Livermore National Lab.(LLNL), Livermore, CA (United States).

Miles Matthew, B., Michael, H.A. and Johnny, S., 2014. Qualitative data analysis: A methods sourcebook.

Miloslavskaya, N. and Tolstoy, A., 2019. Internet of Things: information security challenges and solutions. *Cluster Computing*, *22*(1), pp.103-119.

Miloslavskaya, N. and Tolstoy, A., 2019. Internet of Things: information security challenges and solutions. *Cluster Computing*, *22*, pp.103-119.

Minnaar, A., 2020. 'Gone phishing': the cynical and opportunistic exploitation of the Coronavirus pandemic by cybercriminals. *Acta Criminologica: African Journal of Criminology & Victimology*, *33*(3), pp.28-53.

Mir, R. and Greenwood, M., 2021. Philosophy and management studies: A research overview.

Mishra, N. and Pandya, S., 2021. Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review. *IEEE Access*, *9*, pp.59353-59377.

Mishra, S., Anderson, K., Miller, B., Boyer, K. and Warren, A., 2020. Microgrid resilience: A holistic approach for assessing threats, identifying vulnerabilities, and designing corresponding mitigation strategies. *Applied Energy*, *264*, p.114726.

Mishrif, A. and Khan, A., 2023. Technology adoption as survival strategy for small and medium enterprises during COVID-19. *Journal of Innovation and Entrepreneurship*, *12*(1), p.53.

Mishrif, A. and Khan, A., 2023. Technology adoption as survival strategy for small and medium enterprises during COVID-19. *Journal of Innovation and Entrepreneurship*, *12*(1), p.53.

Mishrif, A. Khan, S., 2023. SMEs in the Gulf: Economic resilience and digital transformation after COVID-19. *Middle East Economic Review*, *18*(3), pp.112-130.

Mitlin, D. et al., 2019. Knowledge matters: the potential contribution of the co-production of research to urban transformation, Manchester: University of Manchester.

Modi, C., Patel, D., Borisaniya, B., Patel, A. and Rajarajan, M., 2013. A survey on security issues and solutions at different layers of Cloud computing. *The journal of supercomputing*, *63*(2), pp.561-592.

Mohajan, H.K., 2018. Qualitative research methodology in social sciences and related subjects. *Journal of Economic Development, Environment and People*, *7*(1), pp.23-48.

Molia, H.K. and Gohel, H.A., 2015. Protection of Computer Networks from the Social Engineering Attacks. *Int. J. Adv. Eng. Technol*, *1*(1).

Montalbano, E., 2021. *Researchers: Booming Cyber-Underground Market for Initial-Access Brokers*. [online] Threatpost.com. Available at: <https://threatpost.com/booming-cyber-underground-market-initial-access-brokers/166965/> [Accessed 17 August 2022].

Mouton, F., Leenen, L., Venter, H.S., 2014. Social engineering attack model. Computers and Security, 59, pp.186-209.

Mouton, F., Malan, M. M. and Leenen, L. V. H. S., 2014. Social engineering attack framework. Johannesburg, ISSA'14.

Mrad, R., 2021. United Arab Emirates: Cybersecurity For SMEs In A Post-Covid Era, Mondaq.

Muhammad, T., Munir, M.T., Munir, M.Z. and Zafar, M.W., 2022. Integrative Cybersecurity: merging zero trust, layered defense, and global standards for a resilient digital future. *International Journal of Computer Science and Technology*, *6*(4), pp.99-135.

Munkhdorj, B. and Yuji, S., 2017. Cyber-attack prediction using social data analysis. *Journal of High Speed Networks*, *23*(2), pp.109-135.

Murphy, 2020. Middle East facing ‘cyber pandemic’ as COVID exposes security vulnerabilities, cyber chief says. [Online]

Murphy, M., 2020. Ransomware attacks on healthcare and public agencies: A 2020 review. *Health IT Security Journal*, *9*(4), pp.55-70.

Mutu, N., Vassilev, V. and Tabany, M.R., 2021. Low cost, easy-to-use, IoT and cloud-based real-time environment monitoring system using ESP8266 microcontroller. *International Journal of Internet of Things and Web Services*, *6*, pp.1-44.

Mwita, K., 2022. Strengths and weaknesses of qualitative research in social science studies. *International Journal of Research in Business and Social Science (2147-4478)*, *11*(6), pp.618-625.

Nadeau, M., 2017. State of Cybercrime 2017: Security events decline, but not the impact. U.S. State of Cybercrime Survey, 28 July.

Naseer, A., Mir, R., Mir, A. and Aleem, M., 2020. Windows-based Ransomware: A Survey. *Journal of Information Assurance & Security*, *15*(3).

Nayak, J.K. and Singh, P., 2021. *Fundamentals of research methodology problems and prospects*. SSDN Publishers & Distributors.

Neal, M., 2010. When Arab-expatriate relations work well: Diversity and discourse in the Gulf Arab workplace. Team Performance Management: An International Journal, 16(5/6), pp.242-266.

Nieles, M., Dempsey, K. and Pillitteri, V.Y., 2017. An introduction to information security. *NIST special publication*, *800*(12), p.101.

Niemimaa, M., 2024. Incorrect compliance and correct noncompliance with information security policies: A framework of rule-related information security behaviour. *Computers & Security*, *145*, p.103986.

Norman, D., Smith, A., Perry, J., 2015. Understanding cybercrime behaviour using protection motivation theory. *Information and Computer Security*, *23*(4), pp.478-495.

Norman, P., Boer, H., Seydel, E.R. and Mullan, B., 2015. Protection motivation theory. *Predicting and changing health behaviour: Research and practice with social cognition models*, *3*, pp.70-106.

O'Kane, P., Sezer, S., Carlin, D., 2018. Malware evolution and attacker tactics: A survey of advanced persistent threats. *Computers and Security*, 72, pp.1-27.

OECD, 2016. Entrepreneurship, SMEs and Local Development in Abu Dhabi, s.l.: OECD.

OECD, 2019. Digital Security and Data Protection in SMEs. OECD.

Ofosu-Ampong, K., 2021. Determinants, barriers and strategies of digital transformation adoption in a developing country Covid-19 era. *Journal of Digital Science*, *3*(2), pp.67-83.

O'Kane, P., Sezer, S. and Carlin, D., 2018. Evolution of ransomware. *Iet Networks*, *7*(5), pp.321-327.

Owusu, G.M.Y., Koomson, T.A.A., Alipoe, S.A. and Kani, Y.A., 2021. Examining the predictors of fraud in state-owned enterprises: an application of the fraud triangle theory. *Journal of Money Laundering Control*.

Owusu, G.M.Y., Koomson, T.A.A., Alipoe, S.A. and Kani, Y.A., 2022. Examining the predictors of fraud in state-owned enterprises: an application of the fraud triangle theory. *Journal of Money Laundering Control*, *25*(2), pp.427-444.

Pancholi, S. and Strobl, G., 2019. Catch-22: Digital Transformation and Its Impact on Cybersecurity, RSM International Association.

Pandey, N. and Pal, A., 2020. Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. *International journal of information management*, *55*, p.102171.

Pandey, P. and Pandey, M.M., 2021. *Research methodology tools and techniques*. Bridge Center.

Panneerselvam, R., 2014. *Research methodology*. PHI Learning Pvt. Ltd.

Papadopoulos, T., Baltas, K.N. and Balta, M.E., 2020. The use of digital technologies by small and medium enterprises during COVID-19: Implications for theory and practice. *International Journal of Information Management, 55*, p.102192.

Paraskevas, A., 2020. Cybersecurity in travel and tourism: a risk-based approach. *Handbook of e-Tourism*, pp.1-24.

Park, S. and Lee, K., 2021. Improved Mitigation of Cyber Threats in IIoT for Smart Cities: A New-Era Approach and Scheme. *Sensors*, *21*(6), p.1976.

Passeri, P., 2016. Cyber Attacks Statistics. [Online]

Patrick, X., Zou, W. and Xu, X., 2023. *Research Methodology and Strategy Theory and Practice*. UK: Wiley.

Patton, M.Q., 2014. *Qualitative research & evaluation methods: Integrating theory and practice*. Sage publications.

Patton, M.Q., 2014. *Qualitative research & evaluation methods: Integrating theory and practice*. UK: Sage publications.

Pawar, S. and Palivela, H., 2022. LCCI: A framework for least Cybersecurity controls to be implemented for small and medium enterprises (SMEs). *International Journal of Information Management Data Insights*, *2*(1), p.100080.

Peng, T., Leckie, C. and Ramamohanarao, K., 2007. Survey of network-based defence mechanisms countering the DoS and DDoS problems. *ACM Computing Surveys (CSUR)*, *39*(1), pp.3-es.

Piedmont, R.L., 2024. Construct validity. In *Encyclopedia of quality of life and well-being research* (pp. 1332-1332). Cham: Springer International Publishing.

Pillai, S.E.V.S. and Polimetla, K., 2024, February. Mitigating DDoS Attacks using SDN-based Network Security Measures. In *2024 International Conference on Integrated Circuits and Communication Systems (ICICACS)* (pp. 1-7). IEEE.

Pinzaru, F., Zbuchea, A. and Anghel, L., 2020. The Impact of the COVID-19 Pandemic on Business. A preliminary overview. *Strategica. Preparing for Tomorrow, Today*, pp.721-730.

Pipikaite, A. and Davis, N., 2020. Why Cybersecurity matters more than ever during the coronavirus pandemic. In *World Economic Forum*.

Pitropakis, N., Panaousis, E., Giannakoulias, A., Kalpakis, G., Rodriguez, R.D. and Sarigiannidis, P., 2018, September. An enhanced cyberattack attribution framework. In *International Conference on Trust and Privacy in Digital Business* (pp. 213-228). Springer, Cham.

Pohle, A., Villani, E. and Grimaldi, R., 2022. Personnel motivation in knowledge transfer offices: The role of university-level and organizational-level antecedents. *Technological Forecasting and Social Change*, *181*, p.121765.

Ponemon Institute, 2018. Understanding the Value of Information Assets, s.l.: Ponemon Institute.

Pranggono, B. and Arabo, A., 2021. COVID-19 pandemic Cybersecurity issues. *Internet Technology Letters*, *4*(2), p.e247.

Priyono, A., Moin, A. and Putri, V.N.A.O., 2020. Identifying digital transformation paths in the business model of SMEs during the COVID-19 pandemic. *Journal of Open Innovation: Technology, Market, and Complexity, 6*(4), p.104.

Probst, C.W., Hunker, J., Bishop, M. and Gollmann, D. eds., 2010. *Insider threats in cyber security* (Vol. 49). Springer Science & Business Media.

Pu, G., Qamruzzaman, M., Mehta, A.M., Naqvi, F.N. and Karim, S., 2021. Innovative Finance, Technological Adaptation and SMEs Sustainability: The Mediating Role of Government Support during COVID-19 Pandemic. *Sustainability, 13*(16), p.9218.

Pu, G., Qamruzzaman, M., Mehta, A.M., Naqvi, F.N. and Karim, S., 2021. Innovative Finance, Technological Adaptation and SMEs Sustainability: The Mediating Role of Government Support during COVID-19 Pandemic. *Sustainability, 13*(16), p.9218.

Qiu, J., Tian, Z., Du, C., Zuo, Q., Su, S. and Fang, B., 2020. A survey on access control in the age of internet of things. *IEEE Internet of Things Journal*, *7*(6), pp.4682-4696.

Radu, L. D., 2018. Green ICT: some challenges and potential solutions. Acta Oeconomica Universitatis Selye, 7(2), pp. 141-150.

Rafli, M., Nusantara, N.C.A., Putri, E.R., Sari, I.P., Zamzami, N. and Muharroman, A.I., 2024. Information Security Behavior and Compliance with ISO 27001 in IT Companies. *Journal of Digital Business and Innovation Management*, *3*(1), pp.62-76.

Ragab, M.A. and Arisha, A., 2018. Research methodology in business: A starter's guide. *Management and organizational studies*, *5*(1), pp.1-14.

Rawashdeh, A. and Rawashdeh, B., 2023. The effect cloud accounting adoption on organizational performance in SMEs. *International Journal of Data and Network Science*, *7*(1), pp.411-424.

Razali, M.F., Razali, M.N., Mansor, F.Z., Muruti, G. and Jamil, N., 2018, November. IoT honeypot: A review from researcher's perspective. In *2018 IEEE Conference on Application, Information and Network Security (AINS)* (pp. 93-98). IEEE.

Rea-Guaman, M., Calvo-Manzano, J.A. and San Feliu, T., 2018, June. A prototype to manage Cybersecurity in small companies. In *2018 13th Iberian Conference on Information Systems and Technologies (CISTI)* (pp. 1-6). IEEE.

Riemer, K., Ciriello, R., Peter, S. and Schlagwein, D., 2020. Digital contact-tracing adoption in the COVID-19 pandemic: IT governance for collective action at the societal level. *European Journal of Information Systems*, *29*(6), pp.731-745.

Rizvi, A., 2022. Talking about cyber-attacks will boost security, says expert. [Online]

Rogers, R.W., 1975. A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, *91*(1), pp.93-114.

Rogers, R.W., 1983. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In: J.T. Cacioppo and R.E. Petty, eds. *Social Psychophysiology: A Sourcebook.* New York: Guilford Press, pp.153–176.

Rose, A., Rahman, M., Duggal, R., Anderson, K., 2020. Cyber resilience in SMEs: Resource constraints and adaptive capacity. *Journal of Small Business Cybersecurity*, *3*(1), pp.25-39.

Rose, A., Rahman, M., Duggal, R., Anderson, K., 2020. Cyber resilience in SMEs: Resource constraints and adaptive capacity. *Journal of Small Business Cybersecurity*, *3*(1), pp.25–39.

Rosencrane, L., 2022. *Top 10 types of information security threats for IT teams*. Available at: https://www.techtarget.com/searchsecurity/feature/Top-10-types-of-information-security-threats-for-IT-teams [accessed 6 June 2022]

Sadaqat, O., 2021. UAE businesses struggle with ransomware recovery times. Gulf News, 14 June. [online] Available at: https://gulfnews.com

Rosencrane, L., 2022. *Top 10 types of information security threats for IT teams*. Available at: https://www.techtarget.com/searchsecurity/feature/Top-10-types-of-information-security-threats-for-IT-teams

Sadeghi, A.R., Wachsmann, C. and Waidner, M., 2015, June. Security and privacy challenges in industrial internet of things. In *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)* (pp. 1-6). IEEE.

Said, J., Alam, M., Ramli, M. and Rafidi, M., 2017. Integrating ethical values into fraud triangle theory in assessing employee fraud: Evidence from the Malaysian banking industry. *Journal of International Studies*, *10*(2).

Salahdine, F. and Kaabouch, N., 2019. Social engineering attacks: A survey. *Future Internet*, *11*(4), p.89.

Samira, Z., Weldegeorgise, Y.W., Osundare, O.S., Ekpobimi, H.O. and Kandekere, R.C., 2024. Comprehensive data security and compliance framework for SMEs. *Magna Scientia Advanced Research and Reviews*, *12*(1), pp.043-055.

Sargeant, J.M., Brennan, M.L. and O'Connor, A.M., 2022. Levels of evidence, quality assessment, and risk of bias: evaluating the internal validity of primary research. *Frontiers in Veterinary Science*, *9*, p.960957.

Saunders, M. and Lewis, P., 2017. *Doing research in business and management*. Pearson.

Saunders, M., Lewis, P.H.I.L.I.P. and Thornhill, A.D.R.I.A.N., 2007. Research methods. *Business Students 4th edition Pearson Education Limited, England*.

Saunders, M.N., Lewis, P., Thornhill, A. and Bristow, A., 2015. Understanding research philosophy and approaches to theory development.

Schuchter, A. and Levi, M., 2016. The fraud triangle revisited. *Security Journal*, *29*(2), pp.107-121.

Seemma, P. S., Nandhini, S. and Sowmiya, M., 2018. Overview of Cyber Security. International *Journal of Advanced Research in Computer and Communication Engineering, 7*(11), pp. 125-128.

Sena, V. and Bhaumik, S., 2021. Firm strategies under Covid-19 induced uncertainty: implications for policy. In *Productivity and the Pandemic* (pp. 32-45). Edward Elgar Publishing.

Sergi, B.S., Popkova, E.G., Bogoviz, A.V. and Ragulina, J.V., 2019. Entrepreneurship and economic growth: the experience of developed and developing countries. In *Entrepreneurship and Development in the 21st Century*. Emerald publishing limited.

Seth, D., Najana, M. and Ranjan, P., 2024. Compliance and regulatory challenges in cloud computing: a sector-wise analysis. *International Journal of Global Innovations and Solutions (IJGIS)*.

Sharevski, F. ed., 2018. *Mobile Network Forensics: Emerging Research and Opportunities: Emerging Research and Opportunities*. Germany: IGI Global.

Sharma, A.C., Gandhi, R.A., Mahoney, W., Sousan, W. and Zhu, Q., 2010, August. Building a social dimensional threat model from current and historic events of cyber attacks. In *2010 IEEE Second International Conference on Social Computing* (pp. 981-986). IEEE.

Sharma, N., Oriaku, E. A. and Oriaku, N., 2020. Cost and Effects of Data Breaches, Precautions, and Disclosure Laws. *International Journal of Emerging Trends in Social Sciences, 8*(1), pp. 33-41.

Sharpe, R. (2021). *The importance of digital communication competence in the competitive advantage context of the UK professional business sector*. University of Salford (United Kingdom).

Shepherd, D., 2022. *Rise of Ransomware Attacks on Businesses in the UAE in 2021.* Available at: https://www.tahawultech.com/news/rise-of-ransomware-attacks-on-businesses-in-the-uae-in-2021/

Shorey, T., Subbaiah, D., Goyal, A., Sakxena, A. and Mishra, A.K., 2018, September. Performance comparison and analysis of slowloris, goldeneye and xerxes ddos attack tools. In *2018 International*

Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 318-322). IEEE.

Shouk, M. and Eraqi, M., 2015. Perceived Barriers to E-Commerce Adoption in SMEs in Developing Countries: The Case of Travel Agents in Egypt. Int. J. Serv. Oper. Manag., 21(332).

Siddiqui, S., 2016. *Cognitive artificial intelligence–a complexity based machine learning approach for advanced cyber threats* (Master's thesis, ACM (IWSPA)).

Silverman, D., 2021. Doing qualitative research.

Singh, P., 2020. The Survival of UAE SMEs in A Post COVID-19 Digital Economy. [Online]

Siponen, M.T. and Oinas-Kukkonen, H., 2007. A review of information security issues and respective research contributions. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *38*(1), pp.60-80.

Smith, L., 2019. *Fordney's Medical Insurance-E-Book*. UK: Elsevier Health Sciences.

Solms, R. v. and Niekerk, J. v., 2013. *From information security to cyber security. Computers and Security, 38*(2013), pp. 97-102.

Sommestad, T., Karlzén, H. and Hallberg, J., 2015. A meta-analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security and Privacy (IJISP)*, *9*(1), pp.26-46.

Sonkor, M.S. and García de Soto, B., 2021. Operational technology on construction sites: a review from the Cybersecurity perspective. *Journal of Construction Engineering and Management*, *147*(12), p.04021172.

Stephanidis, C. and Antona, M., 2020. *HCI International 2020 - Posters: 22nd International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings, Part III.* UK: Springer Nature

Sujeewa, G.M.M., Yajid, M.S.A., Azam, S.M.F. and Dharmaratne, I., 2018. The new fraud triangle Theory-Integrating ethical values of employees. *International Journal of Business, Economics and Law*, *16*(5), pp.52-57.

Sulaiman, N.S., Fauzi, M.A., Hussain, S. and Wider, W., 2022. Cybersecurity behaviour among government employees: The role of protection motivation theory and responsibility in mitigating cyber-attacks. *Information*, *13*(9), p.413.

Sulaiman, N.S., Fauzi, M.A., Hussain, S. and Wider, W., 2022. Cybersecurity behavior among government employees: The role of protection motivation theory and responsibility in mitigating cyber-attacks. *Information*, *13*(9), p.413.

Sullivan, C., 2015. The 2014 Sony hack and the role of international law. *J. Nat'l Sec. L. & Pol'y*, *8*, p.437.

Teasley, L., 2023. New Paths of Attacks: Revealing the Adaptive Integration of Artificial Intelligence in Evolving Cyber Threats Targeting Social Media Users and Their Data.

Thekkoote, R., 2024. Factors influencing small and medium-sized enterprise (SME) resilience during the COVID-19 outbreak. *The TQM Journal*, *36*(2), pp.523-545.

Tornatzky, L.G., Fleischer, M., 1990. *The Processes of Technological Innovation.* Lexington, MA: Lexington Books.

Leavitt, H.J., 1965. Applied organizational change in industry: Structural, technological and humanistic approaches. In: J.G. March, ed. *Handbook of Organizations.* Chicago: Rand McNally, pp.1144–1170.

Barney, J., 1991. Firm resources and sustained competitive advantage. *Journal of Management*, *17*(1), pp.99–120.

Rogers, R.W., 1983. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In: J.T. Cacioppo and R.E. Petty, eds. *Social Psychophysiology: A Sourcebook.* New York: Guilford Press, pp.153–176.

Rose, A., Rahman, M., Duggal, R., Anderson, K., 2020. Cyber resilience in SMEs: Resource constraints and adaptive capacity. *Journal of Small Business Cybersecurity*, *3*(1), pp.25–39.

Töytäri, P. and Rajala, R., 2015. Value-based selling: An organizational capability perspective. *Industrial Marketing Management*, *45*, pp.101-112.

Trend Mirco, 2020. Developing Story: COVID-19 Used in Malicious Campaigns, Trend Mirco.

Tully, S. and Mohanraj, Y., 2017. Mobile security: a practitioner's perspective. In *Mobile Security and Privacy: Advances, Challenges and Future Research Directions* (p. 274). Elsevier Syngress.

UAE Government Portal, 2022. SME statistics in the UAE. [online] Available at: https://u.ae

UAE Government, 2017. Dubai cyber security strategy https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/local-governments-strategies-and-plans/dubai-cyber-security-strategy

UAE, 2022. *Small and Medium Enterprises (SMEs)*. [Online]

Usharani, K., Ramesh, B., Prasad, M., 2021. GandCrab ransomware: Techniques, propagation and mitigation. *International Journal of Computer Applications*, *175*(23), pp.10-18.

Usharani, S., Bala, P.M. and Mary, M.M.J., 2021. Dynamic analysis on crypto-ransomware by using machine learning: gandcrab ransomware. In *Journal of Physics: Conference Series* (Vol. 1717, No. 1, p. 012024). IOP Publishing.

Vadiveloo, J. et al., 2016. Cyber Risk for Small and Medium-Sized Enterprises, University of Connecticut.

Vance, A., Siponen, M. and Pahnila, S., 2012. Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3-4), pp.190-198.

Venkatesha, S., Reddy, K.R. and Chandavarkar, B.R., 2021. Social engineering attacks during the COVID-19 pandemic. *SN computer science*, *2*, pp.1-9.

Vrhovec, S. and Mihelič, A., 2021. Redefining threat appraisals of organizational insiders and exploring the moderating role of fear in cyberattack protection motivation. *Computers & Security*, *106*, p.102309.

Vu, T.T.N., 2021. Understanding validity and reliability from qualitative and quantitative research traditions. *VNU Journal of Foreign Studies*, *37*(3).

Wang, A., Chang, W., Chen, S. and Mohaisen, A., 2018. Delving into internet DDoS attacks by botnets: characterization and analysis. *IEEE/ACM Transactions on Networking*, *26*(6), pp.2843-2855.

Wang, A.J.A., 2005, March. Information security models and metrics. In *Proceedings of the 43rd annual Southeast regional conference-Volume 2* (pp. 178-184).

Wang, Q., Su, M., Zhang, M. and Li, R., 2021. Integrating digital technologies and public health to fight Covid-19 pandemic: key technologies, applications, challenges and outlook of digital healthcare. *International Journal of Environmental Research and Public Health*, *18*(11), p.6053.

Wang, Z., Zhu, H. and Sun, L., 2021. Social engineering in Cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *Ieee Access*, *9*, pp.11895-11910.

Watfa, M., 2016, August. Cloud computing and E-learning: Potential pitfalls and benefits. In *2016 Sixth International Conference on Innovative Computing Technology (INTECH)* (pp. 140-144). IEEE.

Weick, K.E. and Sutcliffe, K.M., 2015. *Managing the unexpected: Sustained performance in a complex world*. John Wiley & Sons.

Wendt, C., Adam, M., Benlian, A. and Kraus, S., 2021. Let's connect to keep the distance: How SMEs leverage information and communication technologies to address the COVID-19 crisis. *Information Systems Frontiers,* pp.1-19.

Whiteman III, J.R., 2017. *Social engineering: Humans are the prominent reason for the continuance of these types of attacks* (Doctoral dissertation, Utica College).

Wolf, W., 2010. *High-performance embedded computing: architectures, applications, and methodologies*. Elsevier.

Woolward, M., 2017. Risk-based approaches to Cybersecurity. *Risk Management*, *64*(4), pp.8-10.

Yamaguchi, S., 2022. Research and Development of Botnet Defence System. In *International Conference on Human-Computer Interaction* (pp. 433-445). Springer, Cham.

Yan, Q., Yu, F.R., Gong, Q. and Li, J., 2015. Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges. *IEEE communications surveys & tutorials*, *18*(1), pp.602-622.

Yan, Z., Gao, G., 2007. Social engineering through relationship exploitation. *Journal of Computers*, *2*(3), pp.88-95.

Younies, H. and Al-Tawil, T. N., 2020. Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE). *Journal of Financial Crime,* 1(1).

Younies, H. and Na, T., 2020. Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE). *Journal of Financial Crime*.

Younies, H. and Na, T., 2020. Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE). *Journal of Financial Crime*, *27*(4), pp.1089-1105.
Younies, H. and Na, T., 2020. Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE). *Journal of Financial Crime*, *27*(4), pp.1089-1105.
Younies, H. and Na, T., 2020. Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE). *Journal of Financial Crime*, *27*(4), pp.1089-1105.
Zahra, S.R. and Chishti, M.A., 2019, January. Ransomware and internet of things: A new security nightmare. In *2019 9th international conference on cloud computing, data science & engineering (confluence)* (pp. 551-555). IEEE.
Zaidan, E., 2017. Analysis of ICT usage patterns, benefits and barriers in tourism SMEs in the Middle Eastern countries: The case of Dubai in UAE. *Journal of Vacation Marketing*, *23*(3), pp.248-263.
Zargar, S.T., Joshi, J. and Tipper, D., 2013. A survey of defencdefence mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE communications surveys & tutorials*, *15*(4), pp.2046-2069.
Zarrouk, H., Sherif, M., Galloway, L. and El Ghak, T., 2020. Entrepreneurial orientation, access to financial resources and SMEs' business performance: The case of the United Arab Emirates. *The Journal of Asian Finance, Economics, and Business, 7*(12), pp.465-474.
Zarrouk, H., Sherif, M., Galloway, L. and El Ghak, T., 2020. Entrepreneurial orientation, access to financial resources and SMEs' business performance: The case of the United Arab Emirates. *Journal of Asian Finance, Economics and Business*, *7*(12), pp.465-474.
Zawya, 2022. Check Point Research: Cyberattacks increased by 50% globally and by 71% in the UAE in 2021. [Online]
Zawya.com, 2022. *Rise of ransomware attacks on businesses in the UAE in 2021: IBM Security Report.* Available at: https://www.zawya.com/en/press-release/rise-of-ransomware-attacks-on-businesses-in-the-uae-in-2021-ibm-security-report-lxtp02mv.
Zhang, C. and Green, R., 2015, April. Communication security in internet of thing: preventive measure and avoid DDoS attack over IoT network. In *Proceedings of the 18th symposium on communications & networking* (pp. 8-15).
Zhang, Y., Kasahara, S., Shen, Y., Jiang, X. and Wan, J., 2018. Smart contract-based access control for the internet of things. *IEEE Internet of Things Journal*, *6*(2), pp.1594-1605.
Zhang, Y., Yang, L.T., Zhou, Y. and Kuang, W., 2010. Information security underlying transparent computing: Impacts, visions and challenges. *Web Intelligence and Agent Systems: An International Journal*, *8*(2), pp.203-217.
Zhou, B. and Pei, J., 2008, April. Preserving privacy in social networks against neighbourhood attacks. In *2008 IEEE 24th International Conference on Data Engineering* (pp. 506-515). IEEE.

Zkik, K., El Hajji, S. and Orhanou, G., 2019. Design and Implementation of a New Security Plane for Hybrid Distributed SDNs. *J. Commun.*, *14*(1), pp.26-32.

Žukauskas, P., Vveinhardt, J. and Andriukaitienė, R., 2018. Philosophy and paradigm of scientific research. *Management culture and corporate social responsibility*, *121*.

Zulkurnain, M., Sulaiman, S., Zainuddin, S., 2015. Human factors in social engineering attacks. *International Journal of Digital Security*, *6*(1), pp.41-49.

Zutshi, A., Mendy, J., Sharma, G.D., Thomas, A. and Sarker, T., 2021. From challenges to creativity: enhancing SMEs' resilience in the context of COVID-19. *Sustainability, 13*(12), p.6542.

APPENDICES

Appendix A: Consent Form

Participant Name: _____

Topic of the Research: Impact and Legacy of the COVID-19 related digital adoption on information security management in SMEs operating in Abu Dhabi

Your participation in this study is highly valued. The study aimed to analyses the impact of post-COVID digital adoption on ISM in SMEs of Abu Dhabi.
If you desire further information regarding the findings of this study, kindly contact me via phone or email at the address provided below:

Email: Mmmal-mulla@lancashire.ac.uk

Name of Investigator: Mahra Al Mulla

Please read and sign the consent statements below:

1. I give my consent as a participant of the current project and all of the information regarding this study has been explained.

2. I acknowledge that:

a) The researcher has informed me that I can withdraw from the research whenever I wish to. Further, I am not obligated to proceed with the remaining questions, and I can request for the removal of my previous responses if unprocessed.

b) I am well informed that my data and anonymity will be protected.

c) I understand that some of my comments may be used in the research study, even though all the information I supply will be anonymous and cannot be used to identify me.

d) I understand that my involvement is entirely optional.

Signature:_____ Date:_____
(Participant)

Appendix B: Research Participant Briefing Sheet

Topic: Impact and Legacy of the COVID-19 related digital adoption on information security management in SMEs operating in Abu Dhabi

Before making a decision on your participation in the research, it is imperative that you possess a comprehensive understanding of the underlying rationale for conducting this study. Furthermore, it is crucial to be cognizant of the expectations placed upon oneself as a participant.
This part will present the information derived from the research investigation. We kindly ask you to conduct a comprehensive and meticulous investigation of the submitted information. You are also welcome to inquire about any questions you may have concerned your decision to participate.

What is the purpose of the study?

The aim of the study is to analyse the impact of post-COVID digital adoption on ISM in SMEs of Abu Dhabi.

Do I have to take part?

Your decision to take part is totally voluntary.

What will happen if I take part?

If you agree to participate in this study, you will be interviewed by the researcher. The duration of the interview is expected to be between 45 and 60 minutes, although it may potentially exceed this timeframe depending on the length of the responses provided. The extent to which one may effectively convey information within the given time range is contingent upon individual effort and ability. Individuals are not bound by any obligation to persist in a situation when they experience discomfort due to the nature of the questions being posed. To facilitate the transcription and subsequent interpretation of the interviews, it is imperative to employ recording techniques.

Will my taking part in this study be anonymous?

Indeed. If you provide consent to participate in the study, interviews will be documented through recording. All personally identifiable information collected during the course of this study will be safeguarded to ensure its confidentiality and prevent public access. The personal information pertaining to your identification will be intentionally concealed in all records. Nevertheless, the research report may

incorporate certain claims from your text without alteration. The researcher intends to analyse the recordings by means of transcription.

What will happen to the results of the research study?

The results of the study are expected to be published in scholarly journals and disseminated through academic conferences. The preservation of secrecy will be maintained consistently. To obtain a copy of the study's conclusions, one can request it by directly contacting the author.

Contact for further information

Mahra Al Mulla
University of Lancashire
Mmmal-mulla@lancashire.ac.uk

Appendix C: Permission Form

Dear xxxxxx,

I am Mahra Mohamed Al Mulla, and I am a student at the University of Lancashire. Currently, I am expected to engage in research work titled "*Impact and Legacy of the COVID-19 related digital adoption on information security management in SMEs Operating in Abu Dhabi"*. To achieve the main objectives and goals of this research, I require data from small to medium enterprises (SMEs).

The study aims to examine the shift observed in business operations and working routines signified by digital adoption and changes in the wake of the pandemic COVID-19. Specifically, the information security management practices within SMEs are the associated challenges due to the pandemic will be the focus. The study is expected to contribute to improving theory and practices related to information security management within SMEs in Abu Dhabi.

I am writing this letter to you because your company fits the criteria of SMEs and data collection required for the study. The data collection requires interacting and obtaining data from the employees working in the company, especially in the IT department. Thus, I request that you provide permission to collect data and conduct research activities within the company and collect data from its employees. I assure you that ethical considerations of research will be kept in mind during research execution and processing.

You are thus requested to read carefully all the points below and mark them before providing permission with your signature at the end.

1	I permit the researcher to interact and obtain data from the employees working in the company (Company Name).	□
2	I am aware that this permission also entails that the researcher would be authorised and remain the owner of the data that is collected from the employees of the company (Company Name).	□
3	I am aware that the researcher would document the research findings and use them for educational and academic purposes only.	□
4	I have been assured that the researcher would comply with the ethical guidelines of conducting research such as obtaining consent from the participants.	□
5	I know that the researcher will anonymise participants' data by using pseudonyms or artificial names to conceal actual identities. However, University of Lancashire does not guarantee that the participants would not be indirectly identifiable.	□
6	I understand that the company name (Company Name). will not be mentioned in the documentation of the research and will be anonymised. However, University of	□

	Lancashire does not guarantee that the company would not be identifiable in an indirect way. OR I grant permission to the researcher to name the company (Company Name). within the documentation of the study and its dissemination.	□
7	I am interested in receiving the final copy of the research document stating the findings of the study. OR There is no need to send the final submitted copy or receive details about the research findings.	□ □
8	I am aware that informed consent will be taken from the participants after educating them about the main purpose of the research and their rights to refuse participation.	□

Signature:

Designation:

Dated:

Appendix D: Interview Questions

Impact and Legacy of the COVID-19 related digital adoption on information security management in SMEs Operating in Abu Dhabi

Tentative Interview Guide

- What were your primary job roles during COVID-19?
- How many years have you worked in your current organisation? How often do you get involved with jobs requiring privacy and security of sensitive data?

Information Security and Management during COVID

1. How does your organisation ensure the security of its data and information?
2. What kind of security threats to information has your organisation faced in the past?
3. What do you think about cybersecurity? Can you explain some of the challenges related to cybersecurity?
4. Please recall your experience during COVID-19, what were your job roles related to information security?
5. Please discuss how you think COVID-19 changed the way you handle information security management.

Challenges Associated with Digital Adoption

6. What were the information security challenges that the organisation faced specifically during the pandemic?
7. What new digital technologies were adopted to ensure information security and management during COVID-19?
8. Please describe the digital technologies or tools that were used during COVID-19. (Prompt: Please share your experience about familiarity with any of these technologies or tools?)
9. In what way have you used any or all of these digital technologies or tools in the past? (Prompt: If you have used any of the digital technologies, please explain how you felt?) (If you have not used any of these digital technologies or tools that your organisation introduced during COVID, please share how did you feel when you first used them?)
10. What kind of challenges became evident when digital technologies were integrated into information security during COVID-19?

Approaches to Address Challenges and Ensure Effectiveness

11. What are your thoughts about the use of digital technologies or digital adoption that occurred during COVID-19? (Prompt: What are you suggestion about the way challenges associated to digital adoption are addressed in your organisation?)

12. Why do you think the organisation adopted digital technologies? What did they do to ensure its effectiveness for information security and management?

13. Please share your experience with these digital technologies that were implemented during COVID-19. (Prompt: Please share an event when you faced a challenge and what did you do to address it?)

14. Please discuss how the employees were prepared to use digital tools or technologies during the COVID.

15. What do you think are the prerequisites of digital adoption and its integration into information security management? (Prompt: Please discuss which of these were considered during the digital adoption in your organisation during COVID-19. Why? Why not?)

Impacts of Digital Adoption

16. Please discuss the changes in terms of costs after the new digital technology's integration into your organisation.

17. What kind of changes have you observed in the information security management of your company since the digital adoption in your organisation?

18. Please discuss whether you have observed any changes in the number or the frequencies of security breaches after the new digital technology's integration in your organisation.

19. Please discuss the changes in employee training and awareness programmes after the new digital technology's integration into your organisation.

20. What areas of information security are likely to get impacted by the digital technology integration in your organisation?

21. How do you think the digital technology adoption during COVID-19 for information security and management has impacted your organisation?

Appendix E: Interview Transcript of a Manager in an SME in Abu Dhabi

Information Security and Management during COVID

1: How does your organisation ensure the security of its data and information?

A: " To protect the data we used local servers and the data was protected with strong firewalls. All sensitive information was stored inside the office on the premises and could only be accessed through our company network. This way no sensitive data was exposed to external parties as all the results were stored internally."

2: What kind of security threats to information has your organisation faced in the past?

A: "We had issues with phishing attacks, where hackers copied our email addresses and attempted to send fraudulent messages to customers using their account details. These are some of the main threats we faced."

3: What do you think about cybersecurity? Can you explain some of the challenges related to cybersecurity?

A: " Cybersecurity is important and especially nowadays where everything is connected to the internet. Like many organisations, we have encountered difficulties when it comes to protection of systems particularly when operating from home. The problem of how to secure the remote access and how to make sure the employees are using the right security measures remained a problem."

4: Please recall your experience during COVID-19, what were your job roles related to information security?

A: " When the pandemic happened, my position changed and I had to ensure that the new technologies which were adopted were secure. I collaborated with the IT department to configure VPNs, firewalls, remote access solutions such as AnyDesk and TeamViewer so that all systems should remain safe when employees continue to work remotely."

5: Please discuss how you think COVID-19 changed the way you handle information security management.

A: " COVID-19 taught us how important remote work security was. In response to this we upgraded our firewall systems, adopted VPN solutions and enhanced the awareness of phishing and other security threats. It was also a time for us to reflect about our security posture and enhance it to address new risks presented by the sudden transition to digital work."

Challenges Associated with Digital Adoption

1: What were the information security challenges that the organisation faced specifically during the pandemic?

A: " The largest issue that we came across was the shift to remote work, which created the necessity to guarantee the stability of communication and safeguard information that was being accessed from

different locations than our office. We had to adopt the use of two factor authentication and enhance the firewalls to meet all the remote entry points."

2: What new digital technologies were adopted to ensure information security and management during COVID-19?

A: "We adopted VPNs, upgraded our firewalls, and used Microsoft Teams exclusively for meetings to ensure we kept communications secure. We also enhanced our email security to prevent phishing and other cyberattacks."

3: Please describe the digital technologies or tools that were used during COVID-19. (Prompt: Please share your experience about familiarity with any of these technologies or tools?)

A: "All meetings were arranged through Microsoft Teams to ensure proper communication, as well as security. I was already familiar with it but it became even more important with the advent of the pandemic and everyone working from home. It was seamless, as these tools were already in practise, though we did add layers of security to them."

4: In what way have you used any or all of these digital technologies or tools in the past? (If you have used any of these digital technologies, please explain how you felt?)

A: " I have used Microsoft Teams before, and it seemed even more important during the pandemic. As it focused on having more meetings and interactions, it offered a secure means of doing so. We also used VPNs for connecting to our internal networks for security purpose. I believed that those tools were crucial to sustaining business performance and protection in the crisis."

5: What kind of challenges became evident when digital technologies were integrated into information security during COVID-19?

A: " The main issue was to enforce compliance with security policies in the course of remote connection to the company systems. Some of the workers had to adapt to new security devices such as VPN and remote applications which required time and user training."

Approaches to Address Challenges and Ensure Effectiveness

1: What are your thoughts about the use of digital technologies or digital adoption that occurred during COVID-19? (Prompt: What are your suggestions about the way challenges associated with digital adoption are addressed in your organisation?)

A: " Use of technology during COVID-19 was crucial because operations had to continue regardless of the situation. Nevertheless, in order to meet them, I think that it is crucial to periodically rehearse employees' training in cybersecurity and improve the company's protection means. It is always a process of evolution."

2: Why do you think the organisation adopted digital technologies? What did they do to ensure its effectiveness for information security and management?

A: " The first of the objectives for implementing digital technologies was to enable and support secure work from home. We made them effective by establishing sound security measures and regularly educating the staff on how to use the tools securely and by conducting periodic cheques for risks."

3: Please share your experience with these digital technologies that were implemented during COVID-19. (Prompt: Please share an event when you faced a challenge and what did you do to address it?)

A: " There was one problem we experienced here, the VPN, which got congested when multiple employees used it at the same time. This slowed down the connexion, and we had to upgrade the licence of the server to meet with the increased traffic. After the upgrade, this problem was solved."

4: Please discuss how the employees were prepared to use digital tools or technologies during COVID.

A: " We had our HR team and the operational team to coordinate with the conducting of workshops and training to the employees. We set up frequent meetings to ensure that participants became acquainted with the digital media and were aware of how to employ them safely. We did this weekly and monthly in order not to leave anyone behind in their practise."

5: What do you think are the prerequisites of digital adoption and its integration into information security management? (Prompt: Please discuss which of these were considered during the digital adoption in your organisation during COVID-19. Why? Why not?)

A: " The basic requirements were to make sure that the tools were integrated with our current architecture and to ensure that our employees knew how to use the tools securely. Security had to be the top priority when these tools were to be integrated into the organisation. In terms of technology, we ensured that we use those that have strong security mechanisms such as Microsoft Teams and VPN, and our employees were trained on how to use them."

Impacts of Digital Adoption

1: Please discuss the changes in terms of costs after the new digital technology's integration into your organisation.

A: " The biggest growth was seen in cost and specifically firewalls as well as VPN access points. We also spent on new software tools to accommodate the need for remote work and security improvements, but it was crucial to ensure that the business could function securely."

2: What kind of changes have you observed in the information security management of your company since the digital adoption in your organisation?

A: " After implementing new digital technologies we have observed positive changes in the organisational security. Organisational systems are more secure from cyber threats; and the employees are more conscious of security measures. We have also improved organisational security measures such as use of passwords, two factor authentication and more secure email systems."

3: Please discuss whether you have observed any changes in the number or the frequencies of security breaches after the new digital technology's integration in your organisation.

A: " When we adopted more secure digital technologies, the occurrence of security breaches went down. The enhancement of our firewall systems and positive changes such as utilising VPN cut down on possible risks as well. But as you know, there are always new threats out there, so we continue to watch our systems carefully."

4: Please discuss the changes in employee training and awareness programmes after the new digital technology's integration into your organisation.

A: " Many companies reported an increase in the training frequency after the introduction of new digital technologies. From time to time, we held cybersecurity awareness meetings especially with the increased use of work from home. It was further pointed out that the IT department ensured that everyone got familiar with new security threats such as phishing and how to deal with them."

5: What areas of information security are likely to get impacted by the digital technology integration in your organisation?

A: " I believe that the greatest potential effect is on secure communication and on the ability to access data. As more people started working from home, the focus shifted to providing ways that employees can safely connect to the company's resources and collaborate. We have also observed better control over external risks, such as phishing, due to improved security features."

6: How do you think the digital technology adoption during COVID-19 for information security and management has impacted your organisation?

A: " COVID-19 forced us to implement digital technology to support continued operations while protecting our systems. It also forced us to make changes on the level of security and to reconsider certain strategies of our organisation's protection against cyber threats, which became a positive effect in the long run."

Appendix F: AAP Form 2023

RESEARCH STUDENT REGISTRY ANNUAL ASSESSMENT OF PROGRESS EXERCISE GUIDANCE NOTES & FORMS

Please note the following actions:

STUDENT completes **REPORT A** (End-of-Year Self-Assessment Report), and emails the entire document to each member of their supervisory team.
STUDENT meets whole Supervisory team. **SUPERVISORY TEAM** reviews the AAP document and contributes to completion of **REPORT B**. **DIRECTOR OF STUDIES** forwards the entire document by email to the RDT.
STUDENT meets with the RDT. **RDT** reviews the file, completes **REPORT C** and forwards it by email to help4researchstudent@uclan.ac.uk (copied to the Head of School by exception only).
Progression Board takes place
If remedial work is required, this is carried out over the specified referral period: **STUDENT** sends the remedial work to the supervisory team by the deadline. **DIRECTOR OF STUDIES** updates **REPORT B (Reassessment section)** and forwards the entire document by email to help4researchstudent@uclan.ac.uk and the RDT (copied to the Head of School by exception only).
Reassessment Board takes place

Important changes to this year's AAP exercise

Students are **no longer required** to submit their Progress File or supervisory records for the AAP exercise. Supervisory teams will be responsible for monitoring that students are maintaining their Progress File each year and RDTs will be responsible for monitoring that regular and appropriate supervision has taken place. Students should take their Progress File to the supervisory meeting and their supervisory records to their RDT meeting.
Students on Professional Doctorates will undertake the same AAP exercise from 2019/20 onwards

The RDT Meeting

- If the RDT is a member of a student's Supervisory Team, an alternative RDT from either within or outside of the School is needed.
- RDTs can make informal arrangements to share RDT interview responsibility where necessary.
- This meeting provides students with access to an academic member of staff outside of their supervisory team, to discuss issues of concern. The RDT will also assess whether there are any general issues relating to the research environment that need to be raised with the Head of School.

Students on an Interruption of Studies

- Students who have formally interrupted their studies at the time of the Progression Board will be given an "Interruption" recommendation. The Board will make the decision, on a case-by-case basis, as to whether the student will need to complete the whole AAP exercise on their return to study or complete REPORT E: "Return to Study" on their return.

Students who are approaching their expected submission deadline

- Students approaching their expected submission date who need to enter their final year must indicate this on REPORT A. The Director of Studies confirms in REPORT B whether this request is supported and viable.

Students who have submitted their theses

- Students who have submitted and are awaiting their viva exam or completing amendments after the viva, are exempt from the AAP exercise.

Name of Student: Mahra Mohammed Al Mulla

REPORT A: End-of-Year Student Self-Assessment Report

Provide comments below. Thissection can be expanded as required.

Comment on progress made over this assessment period. Key points to comment on include:

Summarise the work you have undertaken during the year, including your achievements and plans. Students who have recently completed 'Research Programme Approval' or Transfer to PhD can provide a short summary of work undertaken after successful completion of this milestone.

Have you met the research objectives agreed with your supervisory team last year or at the start of your studies

What actions have you taken to meet identified learning and skills development needs and evaluate the training you have undertaken this year

Identify your strengths, weaknesses, opportunities, and problems identified during the year

Do you have the right facilities and support to complete your project successfully

The previous year of my research work has been exceptionally exciting and insightful for me as I have completed several milestones of my doctoral research programme. Initially, I prepared and submitted the research proposal indicating the scope, methodology, and significance of my study. While writing the proposal, it was important to consider a research topic that is worthy to be explored in depth in the context of the UAE such that the outcomes of my study could be valuable in terms of enhancing knowledge on the chosen phenomenon. Considering my background, aptitude, and the need for delving deep into the challenges and opportunities concerning information security management (ISM) in UAE's SMEs to generate new knowledge, I opted for the research topic that focused on assessing the impact of digital adoption on SMEs' ISM in the post-COVID era. It helped me to narrow down the topic to practices, challenges, solutions, and opportunities associated with digital adoption by SMEs to leverage their ISM systems in the specific context of Abu Dhabi. The COVID-19 pandemic expedited the switch from traditional to digital, which led organisations to adapt to new working conditions, especially working from home. However, it affected security systems drastically, making the situation worse for those responsible for systems security since things changed quickly and an increasing number of people started using technology to serve various purposes. Subsequently, the technology-based small and medium-sized enterprises (SMEs) in Abu Dhabi needed to put information security management on top priority. The reason behind this urgent focus on ISM is that cyber threats e.g., ransomware and phishing are growing at a tremendous pace. In this context, SMEs are more likely to be hacked than large businesses. I have focused on assessing the research problem in the context of Abu Dhabi because it has a big problem with internet security and, therefore, choosing it can enhance the significance of my study.

As part of my research work that I have commenced in my DBA programme, I prepared an **RPA form** that described my study in terms of objectives, and significance. An important step to conduct research in the chosen sector of interest, it is important to obtain **ethical approval** from the university. To this end, I prepared a number of documents and got approval from the concerned. These documents included the ethics application form, gatekeeper email sample, consent form, participant information sheet, data protection checklist, debriefing sheet, and the interview guide. I have made effort to prepare **chapter 1** of my dissertation, which discusses research objectives, research questions, research significance, contribution to knowledge and practice, and contribution to methodology sufficiently. Furthering my research work, I initiated **chapter 2** of my dissertation, which intended to develop a comprehensive view of the current state of knowledge and practice of ISM in SMEs by focusing on the phenomenon of digital adoption in the post-COVID circumstances. By reviewing the related literary sources, it became evident that information related to transactions and operations carried out in the business world is prone to threats in many ways. Later, I pursued writing the research **methodology**, which followed Saunders' research onion model comprising research philosophy, approach, strategy, method, sampling technique, data collection, data analysis, and ethical considerations. I had to choose the most appropriate methods and instruments to conduct my study such that they align with the scope, aim, and objectives of my research. Subsequently, I decided to carry out primary

Project plan for the next 12 months. **Provide details of your main objectives and targets for next year, how you are going to progress these, and indicate deadlines.** **<u>If your EXPECTED submission date is within the next 12 months, or has already passed</u>, and you are <u>not</u> on target to submit on time, you must provide notification to the Progression Board that you will be submitting after this date or on your lapse date. Provide an explanation of the work yet to be completed with a timeline. (S*ubmission after your expected submission date must be supported by your supervisors*.)**	
Expected submission date:	30/12/2025
Final lapse date:	30/12/2025

The primary aim of the research is to assess and enhance the information security practices of small and medium-sized enterprises (SMEs) in Abu Dhabi in the context of the COVID-19 pandemic. This involves critically evaluating the current information security practices in SMEs, understanding the challenges they face, identifying and evaluating tools and solutions that can address these challenges in the context of COVID-19-related digital practices, and developing a best practice model to effectively address cyber challenges specific to SMEs.

i. To critically evaluate the information security practices in SMEs in the wake of the COVID-19 pandemic in Abu Dhabi.

ii. To conceptualise the information security challenges in SMEs in the wake of the COVID-19 pandemic in Abu Dhabi.

iii. To identify and evaluate the tools and solutions addressing the information security challenges while adopting COVID-19 related digital practices.

iv. To critique options for addressing the SME cyber challenges with the development of an associated model for best practice.

I think it would take one and half year to complete the research work of my doctoral programme. My dissertation consists of five major sections, i.e. the introductory chapter, the review of literature, the methodology of research, the analysis of data, and conclusion (and recommendations and future research directions). My study is based on qualitative research methods involving semi structured interviews as the research instrument and thematic analysis as the data analysis method. During the next six months, I will carry out the data collection process. In the latter half of my next academic year, I intend to conduct the analysis of data and discussion of the research findings. Then, I aim to write the conclusion and recommendations of my dissertation in the remaining period of my work plan. Meanwhile, I will do the proof-reading and cross-checking of the data used to enhance the credibility of my report.

Proposed date for final submission of thesis:	30/12/2025

Appendix G: AAP Form 2023

ACADEMIC REGISTRY
ANNUAL ASSESSMENT OF PROGRESS EXERCISE GUIDANCE NOTES & FORMS

Please note the following actions:

STUDENT completes **REPORT A** (End-of-Year Self-Assessment Report), and emails the entire document to each member of their supervisory team.
STUDENT meets whole Supervisory team. **SUPERVISORY TEAM** reviews the AAP document and contributes to completion of **REPORT B**. **DIRECTOR OF STUDIES** forwards the entire document by email to the RDT.
STUDENT meets with the RDT. **RDT** reviews the file, completes **REPORT C** and forwards it by email to PGRAdmin@uclan.ac.uk (copied to the Dean of School by exception only).
Progression Board takes place
If remedial work is required, this is carried out over the specified referral period: **STUDENT** sends the remedial work to the supervisory team by the deadline. **DIRECTOR OF STUDIES** updates **REPORT B (Reassessment section)** and forwards the entire document by email to PGRAdmin@uclan.ac.uk and the RDT (copied to the Dean of School by exception only).
Reassessment Board takes place

IMPORTANT

Students should take their **Progress File** (or equivalent) to the supervisory meeting with their supervisors.
Supervisors should forward supervisory records to the RDT along with the AAP forms ahead of the RDT meeting.
Supervisory teams are responsible for monitoring that students are maintaining their **Progress File** (or equivalent) each year.
RDTs are responsible for monitoring that **regular and appropriate supervision** has taken place.
Students on **Professional Doctorate programmes** undertake the same AAP exercise once they move onto Stage 2 – Research Element

The RDT Meeting

- If the RDT is a member of a student's Supervisory Team, an alternative RDT from either within or outside of the School is needed.
- RDTs can make informal arrangements to share RDT interview responsibility where necessary.
- This meeting provides students with access to an academic member of staff outside of their supervisory team, to discuss issues of concern. The RDT will also assess whether there are any general issues relating to the research environment that need to be raised with the Dean of School.

Students on an Interruption of Studies

- Students who have formally interrupted their studies at the time of the Progression Board will be given an "Interruption" recommendation. The Board will make the decision, on a case-by-case basis, as to whether the student will need to complete the whole AAP exercise on their return to study or complete REPORT E: "Return to Study" on their return.

Students who are approaching their expected submission deadline

- Students approaching their expected submission date who need to enter their final year must indicate this on REPORT A. The Director of Studies confirms in REPORT B whether this request is supported and viable.

Students who have submitted their theses

- Students who have submitted and are awaiting their viva exam or completing amendments after the viva, are exempt from the AAP exercise.

Name of Student: Mahra Mohammed Al Mulla

REPORT A: End-of-Year Student Self-Assessment Report

Provide comments below. Thissection can be expanded as required.

Comment on progress made over this assessment period. Key points to comment on include:

Summarise the work you have undertaken during the year, including your achievements and plans. Students who have recently completed 'Research Programme Approval' or Transfer to PhD can provide a short summary of work undertaken after successful completion of this milestone.

Have you met the research objectives agreed with your supervisory team last year or at the start of your studies

What actions have you taken to meet identified learning and skills development needs and evaluate the training you have undertaken this year

Identify your strengths, weaknesses, opportunities, and problems identified during the year

Do you have the right facilities and support to complete your project successfully

In the past year, I have diligently advanced my research on Information Security and Management (ISM) in Small and Medium Enterprises (SMEs) in Abu Dhabi with a focus on changes brought about by the COVID-19 pandemic. This study analyses the current ISM issues in SMEs particularly in the growing trend of digitization. Previous research undertaken includes a review of the literature and the collection of qualitative data from ISM practitioners to construct a best practice model for ISM. Notable this year has been a year filled with successes and failures, as main lessons learnt from supervisors, who helped shape my research processes and findings.

This year, I have accomplished major steps; the most important of them is the successful completion of chapter 5 and assembling of the chapters 1-5, while chapter 6 is in progress. In the first chapter, I discussed the research proposal where I highlighted the importance of ISM in the post-COVID-19 world. Supervisor feedback also stressed the need to ground my research objectives with concrete, realistic ISM issues in the Abu Dhabi case. This feedback was useful in developing Chapter 2, which involved a literature review, where I also examined the academic and industry understanding of ISM. Here, my supervisor's knowledge of current digital risks that SMEs are exposed to helped me to filter out the most essential and relevant sources and thus improve the quality of the chapter. In line with the principles of ethical research practices that were followed throughout the conducted research, approval was obtained from the university's Ethical Committee whereby an Ethics Application was filled. Part of this process was to develop consent forms, participant information sheets and data protection checklists all compliant with the GDPR. These requirements were particularly crucial to get direction from the supervisor to ensure my research was ethical.

In Chapter 3, I chose a mono-qualitative approach, using semi-structured interviews with the executives of SMEs. Supervisor comments highlighted the importance of a good sampling technique, so I employed purposive sampling, focusing on people with rich experience in managing information security. Following this decision, the gathered data was both meaningful and helpful, as advised by the experts. However, during the data collection process, the most difficult part was searching for resources, and I encountered many problems. I had to frequently change companies and pursue ethics approval. While collecting data, I faced several issues that I had faced as some companies refused to allow me to gather data, and some participants withdrew their responses.

Furthermore, the feedback that was received in Chapter 4, which provided the first set of findings, was very useful in enhancing the thematic analysis.

Chapter 5 which presented a preliminary model of best practices in ISM was expanded taking into consideration the suggestions to incorporate the outcome of some recent cybersecurity workshops. This inclusion has expanded the usability of the model, especially in the versatility aspect as regards overcoming new evolving threats related to using digital technology. Further, every chapter contained personal commentaries on supervisors' feedback, which enhanced the organisation and effectiveness of the work, and highlighted the importance of supervision in academic research.

The professional development this year includes training in thematic analysis and cybersecurity frameworks among others. These training sessions not only developed research skills but also served the purpose of my objectives of studying and managing ISM issues. I am also considering to also continue with my training in Data analysis tools to ensure that the analysis conducted is statistically sound in helping me evaluate my findings.

In the last year, I have realized that I am quite flexible and determined to address the difficulties that may occur, for instance, the lack of time for interviews with the participants.

FINAL YEAR PERMISSION (Includes Professional Doctorates)

In line with Academic Regulations, **all students (including Professional Doctorates) are expected to submit their thesis for examination by their Expected submission date.** Continuation beyond the expected submission point must be approved by Research Degrees Board and is subject to a maximum additional period of 12 months registration.

If your EXPECTED submission date is within the next 12 months, and you are not on target to submit on time, you must apply to the Research Degrees Board - Progression Board, for additional time with an explanation of the work yet to be completed with a timeline.

Project plan for the next 12 months.
Provide details of your main objectives and targets for next year, how you are going to progress these, and indicate deadlines.

Expected submission date:	30/12/2025
Final lapse date:	30/12/2025

Project plan up to submission:

Expand as necessary

The coming year is critical in my learning as I aim to work on my dissertation and submit it by the end of the year, 30th of December 2025. My primary objective is to complete Chapter 6, where I will summarize the results and propose recommendations for enhancing ISM in SMEs. The first six months will be spent on the data collection and analysis to strengthen the ISM best practices model. After that, I will focus on writing a conclusion and doing all the necessary preparations for delivering the final work.

To ensure timely completion, I have set a structured timeline:

Oct 2024 - Mar 2025: Data collection and analysis are fully done. It will also involve the last interviews and the last steps in the thematic analysis according to the supervisor's feedback.

Apr-Jun 2025: Keep an eye on the conclusion and improvements based on the comments given in drafting.

July – Sep 2025: Review all the chapters once more and include any feedback from the supervisory team not included before.

Oct-Dec 2025: Complete the writing process of the dissertation by editing, correcting, formatting and submitting by 30th December 2025.

Thus, by repeating communications with my supervisors, I am sure that I will achieve these goals and meaningfully contribute to the development of the ISM in the SME discipline. They provided me with feedback that helped me decide what my next steps should be in terms of research as well as in terms of producing material that is valuable and of high quality.