Int. j. inf. tecnol.
https://doi.org/10.1007/s41870-024-02288-w

ORIGINAL ARTICLE

A value driven framework for cybersecurity innovation in transportation and infrastructure

Lampis Alevizos[1] · **Lalit Bhakuni**[2] · **Stefan Jäschke**[3]

Received: 15 June 2024 / Accepted: 7 November 2024

Abstract This paper introduces a value-driven cybersecurity innovation framework for the transportation and infrastructure sectors, as opposed to the traditional market-centric approaches that have dominated the field. Recontextualizing innovation categories into sustaining, incremental, disruptive, and transformative, we aim to foster a culture of self-innovation within organizations, enabling a strategic focus on cybersecurity measures that directly contribute to business value and strategic goals. This approach enhances operational effectiveness and efficiency of cyber defences primarily, while also aligns cybersecurity initiatives with mission-critical objectives. We detail a practical method for evaluating the business value of cybersecurity innovations and present a pragmatic approach for organizations to funnel innovative ideas in a structured and repeatable manner. Lastly, shifting the focus from general market appeal to sector-specific needs, our framework provides cybersecurity leaders with the strategic cyber-foresight necessary for prioritizing impactful initiatives, thereby making cybersecurity a core business enabler rather than a burden.

Keywords Innovation · Cybersecurity · Framework · Disruptive · Sustaining · Incremental · Breakthrough · Transportation · Infrastructure · Value-driven

1 Introduction

Cybersecurity in transportation and infrastructure sectors nowadays is crucial for the operational integrity of systems in modern society. It not simply about protecting asset confidentiality, integrity, and availability (CIA), rather it goes beyond that [1]. These sectors are increasingly become interconnected and even reliant on digital technologies, facing rapidly expanding cyber threats [2]. Therefore, a re-evaluation of the innovation strategies employed to protect such critical infrastructure becomes imperative [3].

Historically, cybersecurity innovation has largely been influenced by market-driven forces, often highlighting the development of solutions with broad commercial applicability. Although such an approach has undeniably led to significant technological advances, it does not always align with the specific needs and value propositions in the cybersecurity domain and within self-innovating organizations in the transportation and infrastructure sectors. These industries require a framework for cybersecurity innovation that prioritizes operational continuity, safety, security, and public trust over general market appeal. Oftentimes the cybersecurity innovation in these sectors, originates from within, knowing the details, various aspects, and unique challenges of the business itself [4].

To address this disparity, this paper introduces a business value-driven framework for cybersecurity innovation and cyber-foresight tailored to the unique demands of the transportation and infrastructure sectors. Building upon the established categories of disruptive, transformative,

✉ Lampis Alevizos
lampis@redisni.org

Lalit Bhakuni
lalit.bhakuni@outlook.com

Stefan Jäschke
stefan.jaschke@pm.me

[1] Volvo Group & UCLan, School of Engineering and Computer Science, Amsterdam, The Netherlands

[2] Volvo Group, Amsterdam, The Netherlands

[3] Volvo Group, Gothenburg, Sweden

Published online: 25 November 2024

sustaining, and incremental innovations, we recontextualize them to reflect their contribution to the sectors' business values, such as efficiency, effectiveness, and the capacity to foster a culture of innovation within teams. By doing so, we aim to redirect the focus from market-driven outcomes to innovations that deliver tangible value to the organization's core functions. Innovators often concentrate on fostering interactions between ideas and talents without a long-term vision [5]. In contrast, we extend our focus beyond mere idea generation, emphasizing not only the importance of a prolonged, collaborative journey but also on generating tangible value throughout the process.

The objective of this paper is to critically analyse the traditional market-centric model of innovation and propose an alternative framework that underscores the direct benefits to business operations, especially in sectors where the stakes of cybersecurity breaches are particularly high. To achieve this, we research the theoretical foundations of such an approach, provide a pragmatic methodology to operationalize it within organizations, and discuss its broader implications for strategic decision-making in cybersecurity.

The structure of the paper is as follows: we begin by providing a background and critically discussing the limitations of cybersecurity in the transportation and infrastructure sectors. Next, we detail the theoretical rationale for a value-driven innovation framework, and finally, discuss the practical considerations for its implementation. Thereby, we contribute to the discourse on cybersecurity strategy and offer a pragmatic roadmap for organizations to enhance their defensive capabilities through innovative ways.

Background and literature review

The strategic imperative of cybersecurity in the transportation and infrastructure sectors has been well-documented, with scholars and practitioners acknowledging the increasing sophistication of threats and the need for resilient defence mechanisms [6–8]. Within this context, the transportation and infrastructure sectors face unique challenges, such as the requirement to maintain uninterrupted services and the management of large, complex systems that are often part of the critical national infrastructure (CNI) [9]. Additionally, Knowles et al. [10] conducted a comprehensive review of cybersecurity challenges in critical infrastructure. Their work highlights the unique interdependencies between different infrastructure sectors, which complicates cybersecurity efforts. They argue that these interconnections create a complex web where a security breach in one sector can have cascading effects on others. For instance, a cyberattack on the power grid could indirectly impact transportation systems, water supply, and telecommunications. This interdependency challenges traditional sector-specific security approaches and calls for a more holistic, cross-sector cybersecurity strategy. Furthermore, their research emphasizes the unique challenges posed by legacy systems in industrial control environments, which are common in transportation and infrastructure sectors. These legacy systems often lack modern security features and are difficult to update without disrupting critical services, further complicating cybersecurity efforts.

Mecheva and Kakanakov [11] specifically address cybersecurity innovation in transportation and infrastructure sectors, discussing explicitly sector-specific challenges. They highlight how the increasing connectivity in modern transportation systems expands the attack surface for cyber threats. Their work discusses innovative approaches to securing vehicle-to-everything (V2X) communications, addressing privacy concerns in connected vehicles, and developing resilient traffic management systems. However, they also underline the need for cybersecurity innovations that can operate in real-time and at scale, given the dynamic nature of transportation systems.

The conventional innovation frameworks, while valuable in promoting technological advancement, have been critiqued for their limited scope in addressing the nuanced needs of critical infrastructure [12]. More specifically, the transportation and infrastructure sectors require a focused approach that integrates risk management and operational continuity at its core [13]. This review identifies a gap in current literature where the business value, precisely in terms of operational efficiency and effectiveness, is insufficiently linked with the types of innovation in cybersecurity [14].

Chesbrough et al. [15] introduced the open innovation framework, where collaboration with external partners can bring fresh perspectives and specialized knowledge to internal cyber defence strategies, enhancing the company's ability to respond to evolving threats. However, sharing sensitive information externally can pose security risks, and the focus might divert from internal process optimization, which is crucial for efficiency and effectiveness. Granstrand and Holgersson's work on the other hand [16], propose a more nuanced view of open innovation, particularly relevant to complex systems like those in transportation and infrastructure. They argue that different degrees of openness may be appropriate for different aspects of innovation, which could be principally relevant in cybersecurity where some aspects require high levels of confidentiality. They also propose that effective innovation might require collaboration not just with technology providers, but also with regulators, other infrastructure operators, and even ethical hackers.

Kim's blue ocean strategy [17] encourages creative thinking in identifying unique approaches to cyber defence, potentially leading to more effective internal solutions without direct market competition. Nonetheless, the primary aim of creating market spaces may not align perfectly with internal innovation focused on enhancing current cyber defence capabilities, thus the proposed value driven approach may

be more suitable in this context. Debruyne's [18] customer-centric innovation framework could potentially align closely with the needs of internal users (as 'customers'), subject to repurposing. However, the framework may not fully address the strategic and overarching goals of the organization's cyber defence posture, focusing more on individual user needs. Moreover, the design thinking framework [19] brings a human-centred approach that allows cyber defence solutions to be tailored to the needs of internal stakeholders, but on the other hand, the iterative, empathetic process of design thinking might be time-consuming, resulting in paralysis by analysis phenomena and potentially clashing with the need for rapid implementation in demanding environments. The disruptive innovation framework by Christensen et al. [20] sets the groundwork for potential introduction of new internal technologies or practices that revolutionize a company's cyber defence approach. Nevertheless, disruptive innovations in the cyber defence context within an organization, will necessitate significant adjustment periods. Consequently, this could indicate a time lag between detecting a breach and responding to it. Additionally, Omotayo et al. [21] provide a critical perspective on disruptive innovations in the context of critical infrastructure cybersecurity. Using the water industry as a case study, they argue that while disruptive innovations can offer significant improvements in efficiency and capability, they can also introduce new vulnerabilities. For instance, the adoption of internet of things (IoT) devices in water management systems can improve monitoring and control but also creates new entry points for cyberattacks. Their work shows that in critical infrastructure sectors, a balanced approach to innovation is necessary, one that carefully weighs the benefits of innovative technologies against potential security risks.

Furthermore, there is a growing recognition of the role that sustaining innovation plays in creating an innovative culture within organizations [22]. Therefore, by empowering teams with the responsibility for continual, iterative improvement, sustaining innovation can serve as a catalyst for more ground-breaking initiatives within the cybersecurity domain. However, there is no practical application or a clear road map on how to apply a value driven scoring in the transportation and infrastructure sectors within the cybersecurity domain.

The European Cyber Security Organization's report [23] on organizational culture and innovation provides insights specifically on cybersecurity innovation in transportation and infrastructure. They argue that fostering a culture of innovation requires more than just technological investment; it necessitates creating an environment where employees at all levels feel empowered to contribute ideas and take calculated risks. In the cybersecurity context, this means encouraging security professionals to think creatively about potential threats and solutions, rather than simply following established protocols. Their work also underscores the importance of inclusive innovation practices, and therefore suggests that effective cybersecurity strategies should consider input from a diverse range of stakeholders, including end-users of transportation and infrastructure services.

To synthesize the existing body of work, this paper draws upon original theories of innovation by Christensen et al. [20] and Professor Schumpeter's theory of innovation [24], while also incorporating contemporary insights from cybersecurity and industry-specific sources [25]. This work forges a framework that addresses the gaps identified, while also aligns with the strategic imperatives of the transportation and infrastructure sectors. Ultimately, the evolving cyber landscape and the rise of self-innovating organizations highlights a shift from traditional, market-driven innovation models, which often prioritize scalability and profitability over sector-specific needs. To summarize the literature, we draw Table 1.

2 Framework

This section introduces a framework for cybersecurity innovation, with a unique focus on maximizing business value rather than conventional market-driven metrics. Our proposed framework is based in the principle that the true measure of innovation in cybersecurity lies in its capacity to enhance cyber resilience, mitigate risks, align closely with the strategic objectives of the organizations, improved efficiency, and effectiveness of cyber defences, and provide cyber-foresight. This is contrary to the traditional models that often prioritize market reach, commercialization, and financial profit.

Cyber-foresight is a strategic capability that enables organizations to anticipate, identify, and prepare for future cybersecurity threats and technological trends before those are established [26]. Cyber-foresight is at the core of our value-driven framework. It empowers organizations to proactively identify emergence phenomena and trends in the cyber space, hence cybersecurity strategies can balance between reactive and proactive, in addition to being predictive. This anticipatory stance is imperative in achieving cyber resilience and can even provide a competitive advantage in the transportation and infrastructure sectors.

Therefore, reorienting the innovation process towards these parameters, we present a more relevant and impactful four-stage approach for organizations seeking to drive internal innovation while facing the cyber threat landscape. The four stages, defined and discussed in this order, are as follows: (1) assign innovation category and establish organizational ownership, (2) cybersecurity innovation value proposition scoring, (3) balance resources and risks, (4) execution and value realization. The four stages, along with

Table 1 Summary of literature review

Author and year	Theme	Key points	Identified gaps
Knowles et al. 2015 [10]	Cybersecurity challenges in critical infrastructure	Interdependencies between infrastructure sectors and cascading effects of security breaches	Challenges with legacy systems requiring a more balanced approach to cybersecurity innovation
Mecheva and Kakanakov 2020 [11]	Cybersecurity innovation in transportation and infrastructure	Expanding attack surface due to connectivity of assets within this specific sector	Privacy concerns and need for real-time, scalable solutions
Maglaras et al. 2021 [12]	Conventional cybersecurity innovation frameworks	Valuable for technological advancement but limited in addressing nuanced needs of critical infrastructure	Limited scope in integrating risk management and operational continuity with cybersecurity
Wong et al. 2016 [14]	Business value in cybersecurity innovation	Insufficient linkage of business value (operational efficiency and effectiveness) with types of innovation in cybersecurity	Gap in literature addressing the business value of cybersecurity innovations
Chesbrough et al. 2007 [15]	Open innovation framework	Collaboration with external partners enhances response to threats but poses security risks and may divert focus from internal optimization	Security risks in sharing sensitive information and diversion from internal process optimization
Granstrand and Holgersson 2020 [16]	Nuanced view of open innovation framework	Balancing openness and information protection and collaboration with diverse stakeholders including ethical hackers	Although this nuanced approach includes more relevant stakeholders, and specifically ethical hackers, the same gaps as the open innovation framework (above) remain
Kim 2007 [17]	Blue ocean strategy	Encourages creative, market-space approaches, potentially misaligned with internal cybersecurity needs	Focus on market spaces and does not align with an organisation's internal cybersecurity needs or even enhancements
Debruyne 2014 [18]	Customer-centric innovation	Potential alignment with internal user needs but may not address strategic cybersecurity goals	Framework might not fully address overarching strategic cybersecurity objectives
Van Reine 2017 [19]	Design thinking framework	Human-centred approach beneficial but can lead to analysis paralysis and slow implementation	Time-consuming and may clash with need for rapid deployment in demanding environments
Christensen et al. 2018 [20]	Disruptive innovation	Potential for revolutionary practices but requires significant adjustment periods, leading to delayed responses	Significant adjustment periods needed, causing potential delays in breach response
Omotayo et al. 2021 [21]	Critical perspective on disruptive innovations	The need for a balanced approach to cybersecurity innovation in critical infrastructure becomes evident	No practical framework is proposed
Appio et al. 2021 [22]	Sustaining innovation	Empowers teams for continual improvement, fostering a culture of innovation	Lacks practical application on how to connect all the innovation verticals within cybersecurity
European Cyber Security Organisation 2020 [23]	Organizational culture and cybersecurity innovation	Discussed cybersecurity Innovation beyond technological investment, and, inclusive cybersecurity innovation practices	Highlights the need for cultural aspects of fostering innovation in cybersecurity, nonetheless there is no practical proposal

Table 1 (continued)

Author and year	Theme	Key points	Identified gaps
Christensen et al. 2018 [20], Sweezy 1943 [24] ENISA 2023 [25]	Synthesis of original innovation theories	The original theories of innovation by Christensen and Schumpeter with contemporary cybersecurity insights	Provides the foundation for addressing identified gaps with a new framework
Proposed in this paper	Proposal for value-driven framework	Addresses gaps by aligning cybersecurity initiatives with operational efficiency, business value, and strategic goals	Focus on operational effectiveness, strategic alignment, and business value to enhance cybersecurity measures and resilience

Fig. 1 Value-driven cybersecurity innovation framework

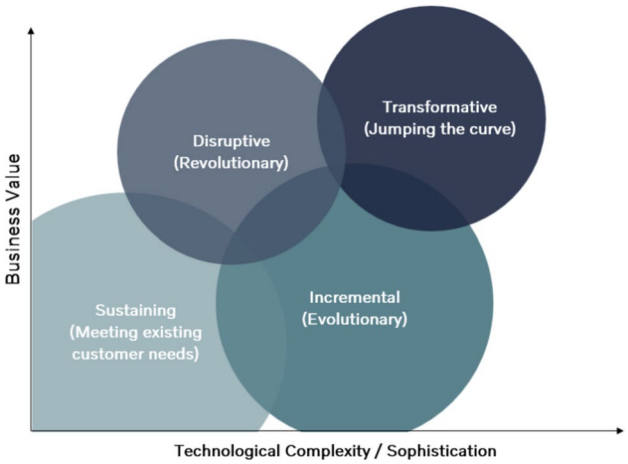

Fig. 2 Value driven innovation aspects

their respective activities, are illustrated in Fig. 1, which is further elaborated upon in this section. These four stages are governed by a cybersecurity innovation forum composed of members with diverse expertise.

2.1 Innovation categorization

The framework details four distinct but complementary aspects of innovation in cybersecurity for the transportation and infrastructure sectors, namely: sustaining, incremental, disruptive, and transformative, visualized in Fig. 2.

Sustaining innovation focuses on refining and enhancing existing processes, while incremental innovation addresses evolving needs through minor yet impactful improvements. Disruptive innovation, on the other hand, introduces radical changes that reshape the cybersecurity landscape of organizations, and transformative innovation leads to fundamental shifts in practices and technologies. The ultimate goal of this framework is to cultivate a culture of self-innovation within organizational teams. Empowering teams to autonomously drive sustaining and incremental innovations, either independently or with support from a dedication cybersecurity

innovation capability that provides tools and guidance, organizations can set the groundwork for innovation at all levels. This strategic approach allows dedicated innovation teams to concentrate their efforts on generating more disruptive and transformative innovations, thereby organizations can achieve a balanced and dynamic innovation ecosystem that responds to current and emerging cyber security challenges.

It is worth noting nonetheless, that excessive focus on any single category within the innovation portfolio can lead to challenges in implementation or diminish the overall impact of the initiative. For instance, a prevalence of incremental ideas might result in diminishing returns, thereby reducing the initiative's relevance over time [4]. Conversely, an abundance of disruptive innovations could present significant integration challenges due to the potential for widespread disruption they entail. We empirically estimate that the optimal composition of an innovation portfolio in the transportation and infrastructure sectors, considering their unique characteristics and as a general framework, a distribution consisting of 45% sustaining, 40% incremental, 10% disruptive, and 5% transformative innovation could serve as an effective initial allocation. Nonetheless this is entirely up to each organization's cultural dynamics, and the maturity of its innovation processes.

2.1.1 Sustaining innovations

Sustaining innovation in cybersecurity, particularly within the transportation and infrastructure sectors, is focused on meeting or even anticipating customer needs [27]. This aspect of innovation is about enhancing the effectiveness and efficiency of existing processes and capabilities of an organization, ultimately focused on extending their business value. Such innovations often arise from systematic efforts like hypothesis testing or thorough intellectual dialogues. For instance, helping stakeholders with innovative technologies or methodologies to understand and address their specific security needs. As a result, this may require developing of a structured and repeatable security process. It may also require developing a unique security solution, which addresses the unique challenge presented by such technologies. The value here lies in increasing efficiency through effective client interfacing. Thus, making sure business needs are understood and met, and providing a clear security journey for clients, backed by factual evidence of the capability to orchestrate and oversee security measures. Sustaining innovations do not require technological complexity or sophistication to be applied, rather they generate improvements and refinements to existing cybersecurity technologies and practices. These innovations maintain and extend the life cycle of current cybersecurity approaches.

2.1.2 Incremental innovations

Incremental innovation refers to evolutionary changes made to meet new customer requirements or adapt to emerging technologies. This aspect introduces a reactive approach to changing needs, producing enhanced innovations to maintain competitiveness [28]. For example, responding to new security service requests from internal stakeholders or customers that may require improving processes to comply with specific regulations or adjusting practices to suit unique operational environments like factory settings with limited internet connectivity. The business value derived from incremental innovation comprises of a collective rise in capabilities maturity, ensuring that all elements of the organization advance in response to new challenges, and the establishment of criteria for assessing innovative technologies before adoption. Incremental innovations are small, evolutionary advancements that contribute to the overall robustness and effectiveness of cybersecurity measures. They can be minor tweaks or enhancements with some degree of technological complexity or sophistication, that cumulatively make significant differences.

2.1.3 Disruptive innovations

Disruptive innovations introduce revolutionary changes, often appearing initially less adequate but eventually providing significant business value. It does not necessitate inflated costs or complex technology but focuses on unlocking new areas of customer engagement or technological application [29]. An example could be developing a new security control framework for industrial control systems (ICS) or enabling service expansion to new business lines. Disruptive innovations also include adopting innovative technologies such as blockchain or artificial intelligence. The business value here lies in streamlining technical security with policymaking, thus providing clear understanding and empowerment in executing security roadmaps and preparing the organization for emerging cyber technologies and trends. Oftentimes breakthroughs happen in this aspect that fundamentally alter the landscape of digital security within an organization. These are often unexpected, coming from outside the traditional cybersecurity domain, and can completely change the rules of the game. For example, the adoption of blockchain technology to secure supply chain data, providing a tamper-proof and transparent ledger for tracking components and materials in the transportation sector [30]. Moreover, the cross-collaborative way of workings in value chains can be seen as a disruptive innovation, initially. Mindset changes in the way of working for a team of cyber threat intelligence, maybe seen as a disruptive innovation. For instance, working every day holistically as a team split into different threat actor verticals, rather than having a designated person

per day monitoring threat actors' activity horizontally. Such innovative ideas can be seen as disruptive in the beginning, nonetheless, over time the business value skyrockets, as the capabilities and teams more effectively and efficiently collaborate to increase cyber resilience while increasing their maturity at the same time.

2.1.4 Transformative innovations

Transformative innovation represents a radical shift in how things are done, often leading to the substitution, or merging of capabilities or technologies. It requires a significant transformation, potentially necessitating a new skill base [31]. For instance, a transformative innovation could be exploring the use of artificial intelligence (AI) in cybersecurity, or the convergence of AI with blockchain and cybersecurity. This type of innovation is about forward-thinking and thought leadership in adopting and utilizing emerging technologies. The business value enters by increased customer trust and brand reputation, as pioneering efforts in cybersecurity can provide a competitive edge and enhance overall cyber resilience. Proactively researching and implementing quantum-resistant cryptographic methods to prepare for the advent of quantum computing, radically altering the approach to data security, is another example of transformative innovation now [32]. Furthermore, an AI-powered predictive maintenance mechanism is another example. Utilizing artificial intelligence to predictively analyse infrastructure health, identifying potential issues before they become critical, thus revolutionizing maintenance strategies. Or using an AI powered cyber threat intelligence pipeline that steers the cyber defences while providing automated cyber threat mitigations [33].

2.2 Cybersecurity innovation value proposition score

Business value in cybersecurity, particularly within the transportation and infrastructure industry, is multifaceted. Primarily revolves around the protection of assets and continuity of operations but it is also about the trust that users place in these critical systems. The value is derived from the effectiveness and efficiency of security measures, their alignment with the organization's strategy, and their contribution to the cyber resilience of the infrastructure. Thereby cybersecurity acts as a business enabler, rather than a showstopper to business objectives. To evaluate the business value of cybersecurity innovations, we propose two models that organisations may use subject to their maturity and expertise for innovation funnelling, namely, a semi-quantitative, and a fully quantitative. Both are multi-dimensional, yet basic models and not mutually exclusive. In fact, they could potentially work synergistically. The latter model considers the cost–benefit analysis, the impact on risk posture, and the enhancement of operational capabilities. As a result, we introduce three key formulas: risk reduction value (RRV), operational efficiency value (OEV), and cost–benefit value (CBV). Each formula captures distinct dimensions of value, providing a quantitative basis for evaluating the efficacy of cybersecurity measures. The former model introduces two additional parameters that can be semi-quantitatively measured, namely, strategic alignment and trust.

2.2.1 Semi-quantitative model

We begin by introducing the term 'Cybersecurity Innovation Value Proposition Score' (CIVPS) inspired by the work of Covin et al. [34], a compound index designed to evaluate ideas across six dimensions: revenue enhancement, cost efficiency, operational efficiency, risk mitigation, trust building potential, and strategic alignment. Each dimension is scored using a consistent scale ranging from 1 to 10, indicative of the estimated potential impact. This evaluation requires the consideration of multiple inputs by the cybersecurity innovation forum, involving a range of stakeholders. Consequently, the process of averaging the scores becomes imperative. The dimensions are depicted in Fig. 3.

- Revenue enhancement potential: potentially innovative ideas are evaluated for their capacity to generate new financial inflows or augment existing revenue streams. This dimension can also be used to assess the potential for delivering value to stakeholders or fulfilling organizational missions or needs.
- Cost efficiency potential: measures an idea's ability to reduce current expenses, extend the life of existing assets, or pre-empt future expenditures, thus positively impacting the organization's cost structure.
- Operational efficiency potential: measures an idea's ability to streamline workflows, reduce/increase capability's

Fig. 3 Cybersecurity innovation value proposition score (CIVPS)

quality deliverables, reduce "time-to-market", or eliminate non-value-adding activities within operational processes.
- Risk mitigation potential: ideas are scrutinized for their potential to address known vulnerabilities, enhance resilience, and reduce both the likelihood and impact of operational disruptions.
- Trust building potential: this dimension considers whether an idea can improve stakeholder perception, organizational perception, either externally or internally, fulfil or surpass customer expectations, and contribute to the organization's overall brand equity.
- Strategic alignment: alignment with the organization's strategic direction provides a dual focus on both the intrinsic value and strategic fit.

Ultimately, scoring should not be the endpoint for all proposals. Often, ideas that do not pass the threshold of the dimensions in the early stages are not inherently deficient but may simply require more elaboration or maturation. These ideas, which may be premature due to the current state of technology or cost considerations, should be returned to their originators for further refinement. With adequate development and a more favourable technological context, these ideas could be reintroduced for consideration in future evaluation rounds.

2.2.2 Quantitative model

Risk reduction value (RRV) measures how much risk is mitigated by a cybersecurity innovation. This can be calculated by estimating the potential loss from cyber threats and the reduction in probability of these threats due to the innovation. PL_{before} represents the potential financial losses due to cybersecurity threats prior to the implementation of a specific innovation. Similarly, let PL_{after} denote the potential losses after the implementation, assuming a decrease due to the innovation's impact. We define $P_{\text{reduction}}$ as the probability reduction of a cybersecurity threat's occurrence as a result of the innovation. The RRV is then given by the equation:

$$RRV = \left(PL_{\text{before}} - PL_{\text{after}}\right) \times P_{\text{reduction}} \tag{1}$$

Operational efficiency value (OEV) quantifies the improvement in operational efficiency. It includes metrics such as reduced downtime or faster threat response times, subject to the context of capability measured. Let $G_{\text{operational}}$ denote the gains in operational efficiency that arise from the innovation, which include reductions in threat detection and response times or the increased automation of security processes, for instance. Let $C_{\text{implementation}}$ represent the total cost of implementing the innovation. Thus, the OEV is calculated as:

$$OEV = \frac{G_{\text{operational}} - C_{\text{implementation}}}{C_{\text{implementation}}} \tag{2}$$

This ratio defines the improvement in operational efficiency in relation to the implementation cost, offering an efficiency measure of the innovation's performance.

Cost–benefit value (CBV) assesses the cost savings against the investment in the cybersecurity measure. It considers both direct costs (e.g., implementation costs) and indirect costs (e.g., people upskilling/training costs or technology stack maintenance). *Total_Savings* aggregate all financial savings yielded by the innovation, including decreased losses from breaches, and improved operational efficiency. Conversely, *Total_Costs* aggregates all expenses associated with the innovation, incorporating initial outlay, maintenance, and any other related costs. The CBV is therefore calculated as:

$$\text{CBV} = \frac{\text{Total\_Savings} - \text{Total\_Costs}}{\text{Total\_Costs}} \tag{3}$$

This formula provides a holistic view of the financial benefits of the cybersecurity innovation against its total cost, summarizing the cost-effectiveness of the investment.

In many cases it is highly likely that innovations may introduce uncertainties. The use of Monte Carlo simulations in our framework provides for a thorough risk analysis and a probabilistic understanding of business value, which is critical for making strategic decisions under uncertainty [35]. For instance, assuming we are evaluating the potential cost savings from preventing cyber incidents over a given period through an innovative blockchain based intrusion prevention system. Let $C_{incident}$ represent the potential costs of cybersecurity incident without the investment on the innovative system. Let $P_{incident}$ be the probability of such an incident occurring within a specific period. Let $C_{investment}$ be the cost of the investment. Let $R_{investment}$ be the reduction in the probability of the incident due to the investment. We run N iterations, where in in each iteration i, we simulate whether an incident occurs based on $P_{incident}$ and $R_{investment}$ and calculcate the cost savings if the incident is prevented. Next, we calculate the average expected savings across all iterations to estimate the business value of the investment.

$$BV_{cyber} = \frac{1}{N}\sum_{i=1}^{N}\left(C_{incident} \times I_{prevented,i} - C_{investment}\right) \tag{4}$$

Let BV_{cyber} represent the estimated business value of the investment. N is the number of iterations in the simulation. Let $C_{incident}$ be the cost of cybersecurity incident. Let $I_{prevented,i}$ represent a binary indicator (0 or 1) for whether an incident is prevented in iteration, and I determined

stochastically based on $P_{incident}$ and $R_{investment}$. Let $C_{investment}$ be the cost of the investment.

In each iteration, $I_{prevented,i}$ s determined by generating a random number and comparing it to the adjusted probability of an incident due to the investment. If the random number is lower than $P_{incident} \times (1 - R_{investment})$ then $I_{prevented,i}$ is set to 1, indicating that an incident would have occurred but was prevented due to the investment. The cost savings for that iteration are then $C_{incident}$ minus $C_{investment}$. By averaging these savings over N iterations, we obtain an estimate of the investment's business value.

This Monte Carlo simulation approach provides for a detailed analysis of the uncertainty and variability associated with cybersecurity risks and the potential savings from investments on innovations, thus, ultimately guide strategic decisions through a quantifiable manner. Together, these formulas form the analytical backbone of the quantitative model, presenting a method for the quantitative evaluation of cybersecurity innovations within this framework.

2.3 Balance resource and risks

In this phase we estimate the necessary effort for implementation in relation to the expected impact. We also estimate the total investment and effort required for an idea to be scaled and adopted within the organization. This assessment is crucial as certain ideas, while potentially straightforward during conceptualization and validation, may need considerable time, resources, or organizational disruption upon deployment. Early recognition of these factors is imperative to establish that the full scope of the resource commitment is clear to all stakeholders. Typically, in this phase, and oftentimes in the earlier phase (2), proposals undergo review for approval and seek endorsement from senior management.

2.3.1 Required effort estimation

To estimate the required effort, it is recommended to formulate estimations in response to queries such as: what quantity of expertise, time, and financial resources are needed to diminish the uncertainties surrounding the concept and to finalize a proof of value (PoV)? What challenges are anticipated in integrating the new concept with existing systems or processes? Are there regulatory approvals or compliance standards that the concept must meet? How extensive is the stakeholder engagement process expected to be? Additionally, what are the projected financial prerequisites for the concept to be embraced organization-wide?

Focusing solely on the initial financial costs needed to investigate an innovative prospect may yield a biased anticipation of the subsequent expansion and integration process. This has the potential to dismiss scenarios where a concept is rapidly validated within weeks, yet the scaling and organizational adoption may span years, demanding substantial financial and manpower investments to fully realize the idea on a larger scale.

2.3.2 Implementation impact estimation

To estimate the implementation impact, it is critical to evaluate whether the idea requires a comprehensive shift in the organizational structure or if its implementation is more localized, thereby response is required to queries such as: does the implementation of the idea need a comprehensive organizational transformation, or is the scope of adoption more limited? Are there requirements for the establishment of new operational processes, governance frameworks, or reporting mechanisms? To what extent will the organization need to modify or upgrade its existing technological infrastructure to accommodate the innovation?

Eventually this is a high-level subjective assessment. Nonetheless, it communicates to the larger organization the attention given to future implications in the innovation process. It also underscores the idea that the quick and iterative pace of innovation does not neglect the assessment of its long-term strategic effects. The results of the assessment may be effectively depicted using a straightforward XY axis graph, as illustrated in Fig. 4.

Innovative ideas positioned in the quadrant of low required effort and low implementation impact typically represent straightforward, achievable targets, known as quick wins. These can be progressed to execution with even moderate initial CIVPS. Conversely, ideas situated within the quadrant requiring high effort and high implementation impact are considered ventures with substantial risk. Such initiatives are advisable only if they show exceptional

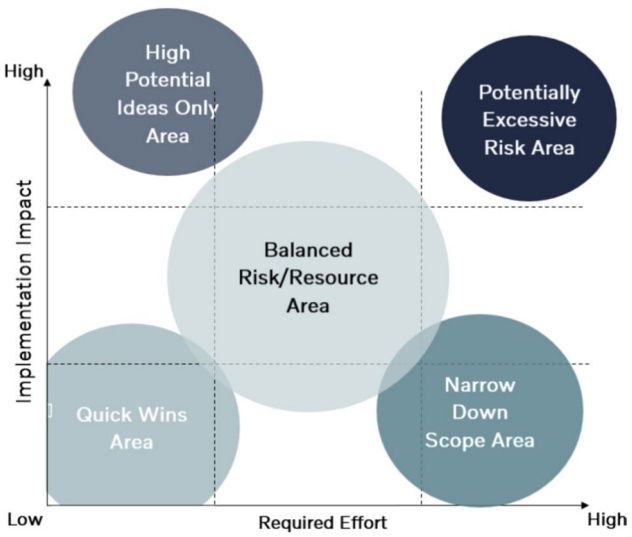

Fig. 4 Cybersecurity innovation ideas road mapping

potential and are among the top-tier disruptive or transformative ideas. Ideas that demand considerable effort but are expected to have a minimal implementation impact call for a scope reassessment prior execution. The strategy should be to find a more contained scope that minimizes the associated risks and supports quicker value realization iteratively and agile. Lastly, ideas requiring minimal effort but offer a significant implementation impact, a "go" signal for execution should be given under conditions upon their extraordinary potential.

2.4 Execution and value realization

In this last stage, the focus shifts to translating vetted cybersecurity innovations into tangible outcomes for the organization. The stage begins with establishing specific timelines, milestones, budget, and risk management strategies following up from the previous stage's outcomes. Next, a project team is formed with clearly defined roles and responsibilities. Typically, a prototype development is crucial, or a minimum viable product (MVP) is essential to test the ideas in real-world scenarios [36]. Several other terminologies and concepts apply at this stage, such as proof of concept (PoC) or proof of value (PoV), subject to organizational needs and dynamics. Moreover, testing and validation alongside stakeholder management naturally should happen at this stage. The team is required to have regular communication with all stakeholders for feedback and alignment while testing and validating the prototype or MVP. The Cybersecurity innovation forum holds a crucial role throughout all stages including execution, providing ongoing support to ensure the innovative solutions are effectively integrated, stakeholders are fully engaged, and the value is ultimately realized. This stage is intentionally designed to be modular, thereby allowing for a high degree of flexibility and customization according to organizational needs and project management methodologies. This design choice enables the framework to accommodate a wide range of innovation execution scenarios, ultimately allowing the outcomes to be both effective and closely aligned with organizational objectives.

3 Discussion

The adoption of a business value-driven framework for cybersecurity innovation represents a paradigm shift for organizations in the transportation and infrastructure sectors. Cyber-foresight enables the strategic alignment of cybersecurity initiatives with business objectives, thereby organizations can better justify investments in cybersecurity, align initiatives with broader strategic goals, ultimately increase stakeholder confidence.

This approach diverges from conventional market-driven strategies, where oftentimes prioritize broad applicability and the potential for commercialization. Such models have driven substantial technological advancements, nonetheless, they may not always address the specific needs of critical infrastructure sectors or dedicated cybersecurity innovation capabilities. Our framework, by contrast, provides a more nuanced approach, where the value of innovation is measured by its direct impact on operational and cost efficiency, risk mitigation, strategic alignment, compliance with sector-specific regulations and brand building equity. This targeted approach is particularly beneficial in sectors where cybersecurity is integral to operational continuity and public safety.

However, certain limitations must be acknowledged. Smaller organizations may face challenges in allocating sufficient resources for disruptive and transformative innovations. Moreover, while we empirically suggested an optimal sector-specific balance through innovation categorization, striking the right balance can be complex and requires ongoing adjustment. Finally, the rapid pace of technological advancements in cybersecurity may require regular reassessment of the framework's relevance.

Conclusions and future research

In this paper, we presented a cybersecurity innovation framework for the transportation and infrastructure sectors based on business value generation rather than one-size-fits-all market driven approach. We provided a structured method for organizations to critically assess and prioritize their cybersecurity initiatives, enable cyber-foresight, help innovative ideas to contribute to the overall strategic goals, eventually enhancing the cyber resilience. The importance on sustaining innovation promotes systematic innovation within teams, encouraging a culture of continuous improvement. The quantitative and semi-quantitative options to measure value provide a data-driven evaluation of cybersecurity initiatives, which aligns them with strategic business objectives and ultimately enhances decision making. Lastly, the strategic focus on transformative and disruptive innovations assists organizations to proactively address emerging cybersecurity threats and adapt to the evolving cyber threat landscape.

Future work is needed to refine these models while exploring the application of this framework in different contexts and scales, particularly in smaller organizations where the resource capacity is an inherent challenge. Another future direction is to assess the implications of the framework for compliance with existing and emerging cybersecurity regulations and standards, and how it can help organizations in meeting these requirements more effectively. Moreover, investigation of methods to improve stakeholder engagement and communication within the framework could be another direction that would ensure all relevant parties

are informed and involved in cybersecurity decision-making processes.

Declarations

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest. This paper reflects the authors own personal views, not necessarily those of Volvo Group.

References

1. Dawson M, Bacius R, Borges Gouveia L, Vassilakos A (2021) Understanding the challenge of cybersecurity in critical infrastructure sectors. Land Forces Acad Rev 26(1):69–75
2. Rajak A, Tripathi R (2024) DL-SkLSTM approach for cyber security threats detection in 5G enabled IIoT. Int J Inf Technol (IJIT) 16:13–20
3. Mhafuzul I, Chowdhury M, Li H, Hu H (2018) Cybersecurity attacks in vehicle-to-infrastructure applications and their prevention. Transp Res Rec 2672(19):66–78
4. Natasha N, Manick S (2017) DSpace @MIT [Online]. https://dspace.mit.edu/bitstream/handle/1721.1/120720/2017-04.pdf?sequence=1&isAllowed=y. Accessed Jan 2024
5. Review HB (2024) Why it's so hard to keep growing. Harvard Bus Rev 88–92
6. Tonn G, Kesan PJ, Zhang L, Czajkowski J (2019) Cyber risk and insurance for transportation infrastructure. Transp Policy 79:103–114
7. Wong KF (2015) Cybersecurity in transportation. In: Protecting our future. Hudson Whitman/Excelsior College Press, pp 111–118
8. Kabanov AS, Gudkov YI, Azarov VN (2019) Problems and prospects of security in the transport sector. In: 2019 international conference "quality management, transport and information security, information technologies" (IT&QM&IS), Sochi
9. Chiappetta A, Cuozzo G (2017) Critical infrastructure protection: Beyond the hybrid port and airport firmware security cybersecurity applications on transport. In: 5th IEEE international conference on models and technologies for intelligent transportation systems (MT-ITS), Naples
10. Knowles W, Prince D, Hutchison D, Disso JFP, Jones K (2015) A survey of cyber security management in industrial control systems. Int J Crit Infrastruct Prot 9(3):52–80
11. Mecheva T, Kakanakov N (2020) Cybersecurity in intelligent transportation systems. Computers 9(4):13
12. Maglaras L, Kantzavelou I, Ferrag MA (2021) Digital transformation and cybersecurity of critical infrastructures. Appl Sci 11(18):8357
13. Moteff J (2005) Defense Technical Information Center (DTIC) [Online]. https://apps.dtic.mil/sti/citations/ADA454038. Accessed 05 Jan 2024
14. Wong EY, Sambaluk NM (2016) Disruptive innovations to help protect against future threats. In: International conference on cyber conflict (CyCon U.S.), Washington, DC
15. Chesbrough HW, Appleyard MM (2007) Open innovation and strategy. Calif Manag Rev 50(1):57–76
16. Grandstrand O, Holgersson M (2020) Innovation ecosystems: a conceptual review and a new definition. Technovation 90–91:102098
17. Kim CW (2005) Blue ocean strategy: from theory to practice. Calif Manag Rev 47(3):105–121
18. Debruyne M (2014) Customer innovation—customer centric strategy for enduring growth. Kogan Page Limited, London
19. Prudhomme PR (2017) The culture of design thinking for innovation. Innov Cult Change Consult Educ 5(2):56–80
20. Christensen CM, McDonald R, Altman EJ, Palmer JE (2018) Disruptive innovation: an intellectual history and directions for future research. J Manag Stud 55(7):1043–1078
21. Omotayo AM, Telukdarie A (2019) Industry 4.0: innovative solutions for the water industry. In: Proceedings of the American society for engineering management international annual conference, USA
22. Appio FP, Frattini F, Petruzzeli AM, Neirotti P (2021) Digital transformation and innovation management: a synthesis of existing research and an agenda for future studies. J Prod Innov Manag 38(1):4–20
23. ECS (2020) Transportation sector report cyber security for road, rail, air, and sea [Online]. https://ecs-org.eu/ecso-uploads/2022/10/5fdb2791553ac.pdf. Accessed June 2024
24. Sweezy PM (1943) Professor Schumpeter's theory of innovation. Rev Econ Stat 25(1):93–96
25. ENISA (2023) European union agency for cybersecurity [Online]. https://www.enisa.europa.eu/news/understanding-cyber-threats-in-transport. Accessed 12 Jan 2024
26. Fischer B, Meissner D, Nyuur R, Sarpong D (2022) Cyber-attacks, strategic cyber-foresight, and security. Trans Eng Manag 69(6):3660–3663
27. Boons F, Montalvo C, Quist J, Wagner M (2013) Sustainable innovation, business models and economic performance: an overview. J Clean Prod 45:1–8
28. Banbury CM, Mitchell W (1995) The effect of introducing important incremental innovations on market share and business survival. Strateg Manag J 16(S1):161–182
29. Nagy D, Schuessler J, Dubinsky A (2016) Defining and identifying disruptive innovations. Ind Mark Manag 57:119–126
30. Hemani, Singh D, Dwivedi RK (2024) Designing blockchain based secure autonomous vehicular internet of things (IoT) architecture with efficient smart contracts. Int J Inf Technol (IJIT)
31. Leicester G (2020) Transformative innovation. In: Transformative innovation a guide to practice and policy for system transition, 2nd edn. Triarchy Press, Axminster, pp 1–14
32. Nadeem M (2024) Analyze quantum security in software design using fuzzy-AHP. Int J Inf Technol (IJIT)
33. Alevizos L, Dekker M (2024) arXiv [Online]. https://arxiv.org/pdf/2403.03265v1.pdf. Accessed Mar 2024
34. Covin JG, Garrett RP Jr, Kuratko DF, Shepherd DA (2015) Value proposition evolution and the performance of internal corporate ventures. J Bus Ventur 30(5):749–774
35. Zhang J (2020) Modern Monte Carlo methods for efficient uncertainty quantification and propagation: a survey. WIREs Comput Stat 13(5):02
36. Nguyen Duc A, Abrahamsson P (2016) Minimum viable product or multiple facet product? The role of MVP in software startups. In: Agile Processes, in Software engineering, and extreme programming