Redesigning Cybersecurity Awareness-Raising and Training Programs: Insights from Professionals on Knowledge, Skills, and Educational Practices

Apostolos Charalambous (Faculty of Pure and Applied Sciences, Open University of Cyprus, Cyprus)

Andriani Piki (School of Science, University of Central Lancashire – Cyprus Campus, Cyprus)

Eliana Stavrou (Faculty of Pure and Applied Sciences, Open University of Cyprus, Cyprus)

Abstract

Purpose

This study aims to examine the perceptions of cybersecurity professionals in order to extract key recommendations for designing effective and impactful security education, training, and awareness (SETA) programs. These programs are intended to address the diverse needs of learners with non-technical backgrounds, as well as IT professionals pursuing specialized training for re/upskilling.

Design/methodology/approach

A survey-based research approach was applied, including both closed and open-ended questions exploring the perceptions of cybersecurity professionals on important aspects pertinent to the design of cybersecurity awareness-raising and specialized training programs, including key knowledge areas and skills, prominent ENISA European cybersecurity skills framework (ECSF) roles, the importance of cyber ranges and key pedagogical considerations.

Findings

The study results suggest that, to be effective, SETA programs must be audience-centric and that the teams responsible for designing them must combine technical expertise, knowledge and skills such as understanding cyber threats, implementing security technologies and incident management, with transferable skills, including communication and adaptability. These findings highlight that SETA teams must include roles with strong technical competencies and pedagogical understanding alike.

Originality/value

The novelty of this study lies in its focus on differentiating SETA programs based on the unique needs of two diverse learner groups, emphasizing the cybersecurity roles, knowledge, skills and pedagogical factors that are important for redesigning awareness-raising and training programs, ultimately leading to a sustainable cybersecurity culture.

Keywords

Cybersecurity culture, SETA, cybersecurity awareness-raising, cybersecurity training, transferable skills, ECSF.

1. Introduction

As the number of cyber threats continues to escalate and become more sophisticated, organizations face increasing challenges in protecting their digital assets (Kandpal *et al.*, 2025) and the privacy, safety, and security of all stakeholders. Considering these challenges, it is imperative to develop a proactive and sustainable cybersecurity culture (Uchendu *et al.*, 2021; Al-Nuaimi, 2024). Central to achieving this culture are Security Education, Training, and Awareness (SETA) programs (Alyami *et al.*, 2023; Trend Micro, 2024; Shillair *et al.*, 2022), which aim to cultivate cybersecurity values and competencies, foster appropriate attitudes and behaviors (Grill et al., 2025; Tran *et al.*, 2025), as well as promote best practices throughout the organization. Despite ongoing efforts to tackle these challenges and the widespread implementation of SETA programs, recent research shows that these programs are not very effective (Hu *et al.*, 2022). Previous work (Charalambous and Stavrou, 2024) began addressing the gaps in SETA programs by exploring which of the cybersecurity career roles, defined in the ENISA European Cybersecurity Skills Framework (ECSF) (ENISA, 2022), collectively provide the required expertise for SETA program development. The findings suggest that both ECSF roles with deep technical competencies and roles adept at pedagogical strategies and communication are imperative, including CISO, Cyber Incident Responder, Cybersecurity Architect, and Cybersecurity Educator. The study further emphasized the importance of designing diversified SETA programs, differentiating clearly between awareness-raising initiatives targeting learners with non-technical background and specialized training programs aimed at IT professionals. Building upon these findings, the current research aims to distinguish between the skills and knowledge required, as well as the instructional approaches that are considered more appropriate for diverse groups of learners. To address this research aim, this study explores and analyzes the perceptions of cybersecurity professionals to extract key recommendations for developing and improving the effectiveness of cybersecurity awareness-raising and training programs targeting non-technical and technical audiences, respectively. By leveraging the insights from this research, all stakeholders (e.g. academia, organizations, policymakers) can gain a deeper understanding of the critical elements that contribute towards formulating effective SETA programs and ultimately a sustainable cybersecurity culture.

The following objectives are formulated:

- Explore how the knowledge and skills required for designing effective cybersecurity awareness-raising compare with those required for specialized training programs.
- Investigate which ECSF roles are essential for designing awareness-raising and training programs.
- Evaluate the perceived importance and effectiveness of utilizing cyber ranges in SETA program development for diverse audiences.
- Explore pedagogical considerations and their perceived impact on the effectiveness of SETA programs.
- Investigate the factors to construct an inclusive and impactful SETA program design team.

This paper is structured as follows: Section 2 presents related work and Section 3 outlines the research methodology employed. Section 4 presents the data analysis providing insights into the knowledge areas, skills, roles, and educational methods identified as critical for SETA program effectiveness. Section 5 critically discusses these findings and Section 6 concludes the paper.

2. Related Work

Cybersecurity awareness-raising and training programs are crucial for promoting a robust organizational cybersecurity culture (Grill *et al.*, 2025). SETA programs aim to educate employees about fundamental cyber threats, encourage safe cybersecurity behaviors, and instill a culture of security within organizations (Grill *et al.*, 2025; Tran *et al.*, 2025). Besides subject-specific knowledge, both human and contextual factors influence cybersecurity behaviors in organizations (Al-Nuaimi, 2024; Godwin, 2025). Hence, to be successful and effective, awareness-raising and training initiatives must be accessible, engaging, and tailored to the audience's specific knowledge level, demographic group, and organizational context to maximize their impact. However, organizations' inability to effectively address cybersecurity incidents and breaches (Gundu *et al.*, 2024) have raised concerns regarding the efficacy of these initiatives. Despite the acknowledged necessity and widespread adoption of SETA programs, their effectiveness often remains limited due to several reasons (Hu *et al.*, 2022) - pedagogical, organizational, and human-oriented.

On the educational front, many programs lack a sound pedagogical foundation featuring generic or policy compliance-driven content, employing non-interactive approaches, or characterized by an inadequate understanding of employee motivation and the dynamics of behavioral change (Alyami *et al.*, 2023; Hu *et al.*, 2021;

Kirova and Baumöl, 2018). The lack of carefully designed education and training curricula, alongside the lack of expertise in tailoring such initiatives to the specific needs of each individual and organization, often lead to superficial educational content with no impact on the sustainable education and training of the workforce. As discussed in previous work (Charalambous and Stavrou, 2024; Uchendu *et al*., 2021), numerous SETA programs have been found to lack the capacity to influence employee behavior effectively or to provide individuals with the requisite knowledge and skills to address emerging cyber threats. The gaps may also be attributed to the lack of a systematic understanding of the nature of SETA programs and the ways in which SETA impacts employees' security-related beliefs or behavioral intentions (Hu *et al*., 2022).

From an organizational leadership angle, many organizations struggle to establish a sustainable cybersecurity culture (Al-Nuaimi, 2024) with many educational efforts being offered as short-term or one-off interventions due to constrained training budgets or failure to appreciate the impact of lifelong learning (Charalambous and Stavrou, 2024). These challenges also limit the provision of effective specialized training programs targeting IT and cybersecurity professionals. Given the diversity of cybersecurity career roles (ENISA, 2022), several needs emerge: to address sector-specific needs and relevant risk profiles, to promote realistic and role-based training programs, and to foster a holistic cybersecurity culture across the organizational hierarchy (Floros *et al*., 2025).

The recent focus on designing micro-credentials to enable life-long learning, some with questionable quality and others with varying depth and coverage (Raj *et al*., 2024), is another limiting factor to achieving engaging learning and ultimately an effective cybersecurity culture. When educational offerings are not coupled with appropriate career guidance, it can challenge organizations and individuals' participation in training (Al-Nuaimi, 2024). Lack of proper understanding of what competences need to be cultivated, may lead individuals and organizations to choose generic over tailored SETA programs which cover only surface-level knowledge and skills and fail to engage employees and instigate appropriate cybersecurity attitudes (Hu *et al*., 2021; Karimnia *et al*., 2022). This further contributes to the growing skills gaps considered as the biggest barrier to business transformation, "with 63% of employers identifying them as a major barrier over the 2025-2030 period" (WEF, 2025, p. 6). Furthermore, keeping up with new policies and regulations being introduced in response to rapid digital transformations and technological advancement (such as GDPR and EU AI Act) necessitates continuous education, training, and re/upskilling (Alyami *et al*., 2023; Stavrou and Piki, 2024; Uchendu *et al*., 2021), not only for cybersecurity professionals but for everyone using digital technology (Armas and Taherdoost, 2025). These gaps have important implications for higher education institutions (Al-Nuaimi, 2024; Armas and Taherdoost, 2025) especially in the context of Master's programs in cybersecurity which demonstrate significant variation in the coverage of technical versus non-technical topics (Stavrou and Furnell, 2025) such as SETA aspects. If graduates are not exposed to the appropriate knowledge and skills, they will not be able to design effective SETA programs.

These observations and the increasing complexity of the cyber threats landscape indicate there is a need for adopting a holistic approach towards the design of SETA programs. Such an approach should bring together several aspects: industry experience; domain expertise on key cybersecurity knowledge areas; instructional design and content development experience; exposure to educational technology for leveraging innovative approaches for learning; and an understanding of innovative pedagogies for engaging diverse audiences and achieving different purposes – from raising awareness among office employees to re/up-skilling cybersecurity professionals. Given the broad range of skills, knowledge, and competencies required for the design of impactful and effective SETA programs, leveraging a collective approach and forming knowledgeable teams that bring together a diverse range of perspectives, skills, and expertise can contribute to the design of more effective SETA programs and, in turn, to the development of a sustainable cybersecurity culture (Al-Nuaimi, 2024; Charalambous and Stavrou, 2024).

3. Methodology

Building on the initial study (Charalambous and Stavrou, 2024) which draws on an in-depth bibliographic review, the current research study gathered primary data to validate initial findings by exploring the perceptions of cybersecurity professionals on prominent themes. We reached out to cybersecurity professionals aiming to capture their perceptions on the knowledge areas, transferable skills, and educational methods which they consider crucial for designing effective SETA programs. Moreover, we investigated their views on associated topics such as how gender diversity in the instructional development process contributes to the effectiveness of such programs and how effective cyber ranges are for different learners. Specifically, the participants were invited to consider the needs of two different target groups: (i) non-IT staff, and (ii) IT/cybersecurity professionals, hence allowing us to capture the distinction between (i) the development of generic cybersecurity awareness-raising programs and (ii) specialized training programs. In the first case, the target audience typically has no/limited knowledge of technical issues, while in the second case the program is designed specifically to re/up-skill individuals with IT/cybersecurity knowledge. By capturing the needs of these diverse groups, the aim was to identify ways for making SETA programs more effective and impactful, guided by the gaps identified in recent literature.

Data collection was conducted using a structured online questionnaire comprising both closed and open-ended questions, allowing for the collection of quantitative and qualitative data, respectively. Closed-ended questions facilitate the generation of measurable and comparable responses, while open-ended questions enabled participants to elaborate on their perspectives and contextualize their views, hence enriching the data and adding contextual depth (Braun and Clarke, 2006; Creswell and Creswell, 2018).

To identify and recruit participants, we employed the snowball sampling technique (Goodman, 1961). We initially reached out to our network, inviting cybersecurity professionals to respond to the questionnaire while also encouraging them to suggest other individuals within their social or professional networks. It was clearly and explicitly communicated that participation is voluntary and anonymous, and that participants can withdraw at any time. The gathered insights were analyzed using descriptive statistics, sentiment analysis and thematic analysis (Braun and Clarke, 2006), allowing for the identification of key trends, differences, and insights across participant responses.

4. Data Analysis

This section presents a detailed analysis of the questionnaire responses. Cybersecurity professionals (n=50) across Europe, and with varying years of experience, responded to the questionnaire. Specifically, 40% of respondents had more than 10 years of professional experience in the field, indicating a strong professional background, 24% had 6-9 years of experience, while the remaining 36% had 5 years of experience or less. The analysis focuses on (i) the cybersecurity knowledge areas required for designing awareness-raising programs for non-IT staff, (ii) the cybersecurity knowledge areas required for designing specialized training programs for IT/cybersecurity professionals, (iii) the transferrable skills needed for constructing effective SETA Programs, (iv) the most prominent educational considerations, (v) the key factors affecting the effectiveness of the teams responsible for developing SETA programs, (vi) the importance of cyber ranges as a means to educate different learners, and finally, (vii) the importance of different ECSF cybersecurity career roles in instructional design.

4.1. Cybersecurity Knowledge Areas for Designing Awareness-Raising Programs

Current research indicates there is an extensive array of thematic areas that cybersecurity professionals responsible for designing awareness-raising programs need to be knowledge about designing effective programs. Nevertheless, cybersecurity professionals are more likely to specialize in a subset of these areas. Hence, study participants were invited to rate these key areas in terms of their importance in relation to the design of cybersecurity awareness-raising programs (Figure 1).

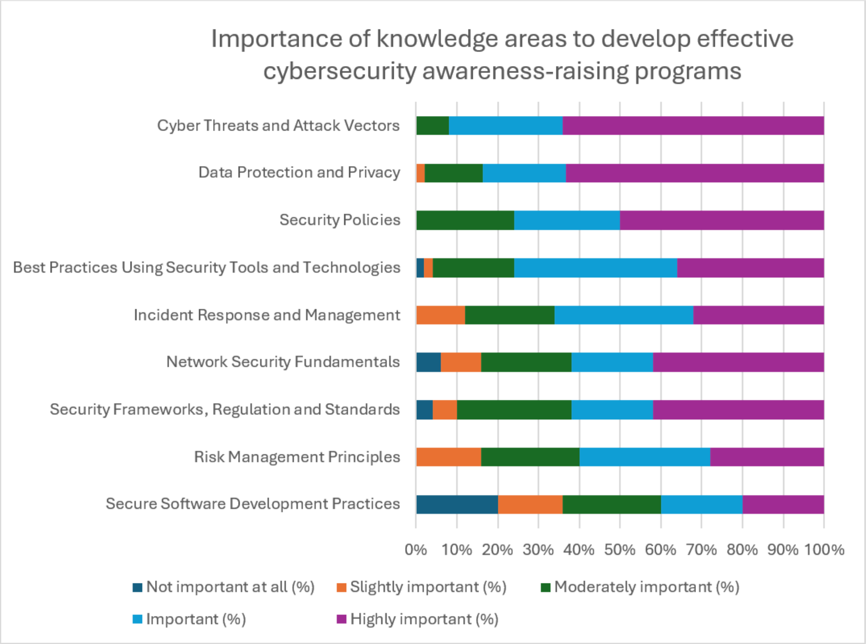


Figure 1: Importance of Knowledge Areas for Designing Cybersecurity Awareness-Raising Programs (%) (Source: Authors own work)

An analysis of the distribution of responses provides a clear indication that certain cybersecurity knowledge areas are, indeed, considered more crucial than others for developing cybersecurity awareness-raising programs for non-IT staff. Participants indicated that the most significant knowledge area is 'Cyber Threats and Attack Vectors' with 92% of respondents considering it to be either 'Highly Important' or 'Important', followed by 'Data Protection and Privacy' (82%). These results show the importance of a comprehensive understanding of cyber threats, common attack methods, and potential consequences in developing relevant educational material and fostering awareness among non-IT employees, empowering them to better recognize cybersecurity incidents. Equally, knowledge on data protection principles and techniques to protect sensitive information is essential for educating employees on the importance of protecting sensitive data, and about data privacy best practices and methods that can be utilized, such as encryption and anonymization.

'Security Policies' and 'Best Practices Using Security Tools and Technologies' were also considered 'Highly Important' or 'Important' by 76% of the participants (with the former receiving a higher percentage of participants (50%) recognizing it as 'Highly Important' compared to the latter (36%)). These results suggest that some participants might perceive these knowledge areas as beneficial but not as critical for the success of cybersecurity awareness-raising programs. Nonetheless, the results reflect the importance placed on communicating clear organizational guidelines, procedures, and behavioral expectations to all employees. At the same time, participants indicated that knowledge on technical concepts and tools is required to design effective awareness-raising programs. Programs that include practical aspects that can empower staff to use tools, apply best practices and be able to recognize and prevent common cybersecurity threats can significantly contribute to the organization's cyber resilience. The remaining knowledge areas received varying ratings with a slightly higher percentage of 'Moderately important' and 'Slightly important' ratings, reaching 28% and 16%, respectively. This finding suggests that participants may perceive some knowledge areas as beneficial but not as critical for the success of cybersecurity awareness-raising programs, considering that knowledge on responding to incidents ('Risk Management Principles'), understanding risk and network security principles ('Risk Management Principles', 'Network Security Fundamentals'), and comprehending cybersecurity regulations and frameworks ('Security Frameworks, Regulation and Standards'), might be too specialized or complex, hence less important for developing awareness-raising programs for non-IT audiences. This observation is further supported when considering the knowledge areas that were rated as 'Not important at all'. A notable 20% of participants did not acknowledge the importance of the 'Secure Software Development Practices' knowledge area, indicating that some professionals might perceive software development practices as less relevant to awareness-raising initiatives targeting non-technical staff.

A notable observation concerns ‘Risk Management Principles’. Although this knowledge area is highly relevant to ‘Cyber Threats and Attack Vectors’ that was rated as the most important knowledge area (with 64% rating it as ‘Highly important’), participants did not rate it with similar levels of high importance with only 28% acknowledging it as ‘Highly Important’. This discrepancy suggests that participants might not fully recognize or appreciate the interconnectedness between understanding cyber threats and the effective management of associated risks. Such a gap indicates a potential area for enhancing cybersecurity awareness programs by explicitly emphasizing how risk management principles can empower non-technical staff to better comprehend, evaluate, and respond to cyber threats within their organizational roles.

Another notable observation is that a few knowledge areas were rated as ‘Not important at all’, including ‘Secure Software Development Practices’ (20%), ‘Network Security Fundamentals’ (6%), ‘Security Frameworks, Regulation and Standards’ (4%), and ‘Best Practices Using Security Tools and Technologies’ (2%). This outcome indicates that professionals generally perceive software development practices and the applicability of technologies as less relevant to awareness-raising initiatives targeting non-technical staff.

4.2. Cybersecurity Knowledge Areas for Designing Specialized Training Programs

Participants were subsequently invited to consider the importance of the knowledge areas in the context of designing specialized cybersecurity training programs targeting trainees who are IT or cybersecurity professionals (Figure 2).

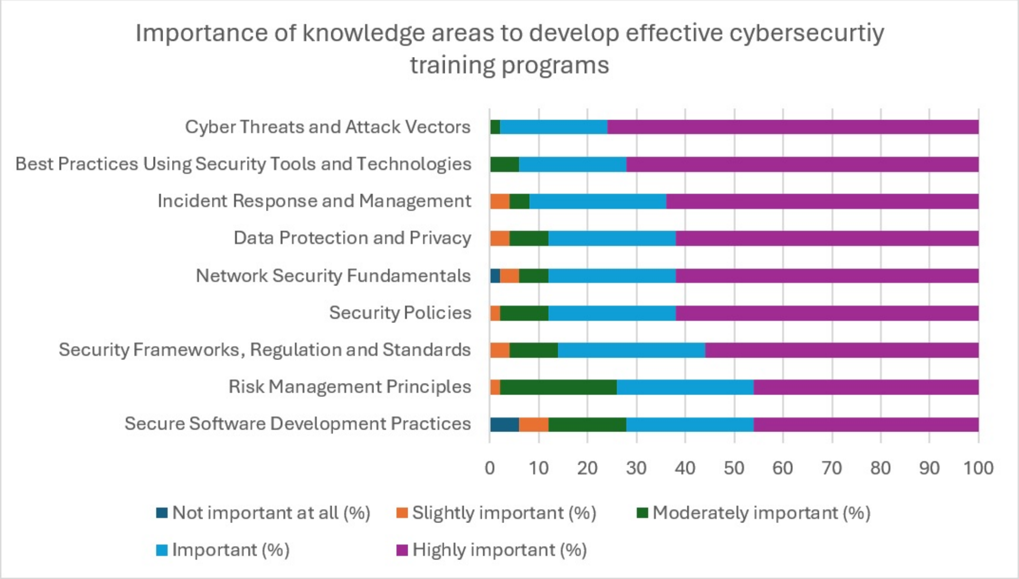


Figure 2: Importance of Cybersecurity Knowledge Areas for Designing Specialized Training Programs (%) (Source: Authors own work)

An initial observation is that the results in this case depict a clearer and more orderly view. In each area, the majority of the participants assigned a ‘Highly important’ rating (46-76%) followed by ‘Important’ (22-30%). This demonstrates that when it comes to developing programs for technical staff, the instructional designers themselves should be knowledgeable across various areas. This was expected given that the audience of training programs is expected to have technical expertise and specialized training needs, compared to the general audience of awareness-raising programs. Specifically, ‘Cyber Threats and Attack Vectors’ received the highest rating, with 98% of respondents recognizing its importance (76% as ‘Highly Important’). This indicates that understanding, recognizing and mitigating cyber threats should be a top priority in cybersecurity training programs, empowering trainees to build relevant competences. Similarly, ‘Best Practices Using Security Tools and Technologies’ and ‘Incident Response and Management’ received ratings of 94% and 92%, respectively, highlighting their perceived criticality for designing specialized training programs. The findings emphasize that possessing practical knowledge and hands-on experience with security tools is crucial for professionals tasked with safeguarding their organizations against cyber threats. Additionally, the results highlight the importance of preparedness in effectively managing and responding to cybersecurity incidents. Professionals tasked with designing relevant training programs should demonstrate relevant knowledge and skills so they can effectively inform their training programs design.

Findings also provide valuable observations regarding the importance of non-technical knowledge areas rated as ‘Important’ or ‘Highly important’ (86-88%), placing an emphasis on the significance of clearly communicating organizational guidelines (‘Security Policies’), and the necessity of safeguarding sensitive data and other organizational assets through compliance and best practices (‘Data Protection and Privacy’, ‘Security Frameworks, Regulation and Standards’). The knowledge areas of ‘Secure Software Development Practices’ and ‘Risk Management Principles’ received comparatively lower importance ratings (72% and 74%, respectively). These findings suggest that while participants recognize these areas as valuable, they perceive them as somewhat less immediately critical for developing SETA programs, compared to other more directly technical knowledge areas. Specifically, ‘Secure Software Development Practices’ might be considered more relevant primarily for professionals directly involved in software engineering or application development roles, rather than the broader cybersecurity workforce. Similarly, the slightly lower emphasis placed on ‘Risk Management Principles’ indicates that some professionals might view strategic risk assessment as a managerial or specialized function rather than a universally essential skill within the technical cybersecurity community.

4.3. Transferable Skills for SETA Programs

While technical skills and specialized knowledge areas are key, it is increasingly emphasized that professionals must also demonstrate an array of transferrable or soft skills. The latest ‘Jobs of the Future’ report states that “workers must balance hard and soft skills to thrive in today’s work environments” (WEF, 2025, p.35). Charalambous and Stavrou (2024) identified a list of transferable skills that professionals need for creating effective SETA programs and fostering a robust cybersecurity culture. Figure 3 illustrates the importance of these skills as perceived by cybersecurity professionals in the current study.

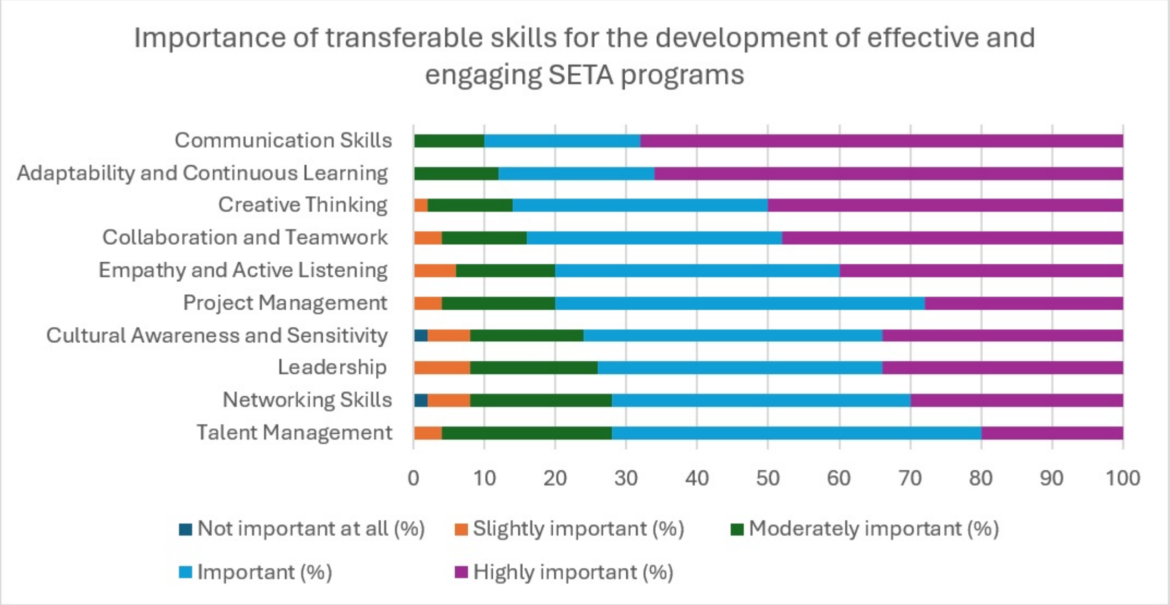


Figure 3: Importance of Transferable Skills (%) (Source: Authors own work)

The significance of transferable skills in designing effective and engaging SETA programs is evident from the survey results. All transferable skills were rated as ‘Important’ or ‘Highly Important’ (ranging from 72% to 90%), reinforcing the critical role these non-technical competencies play in designing effective SETA programs. ‘Communication Skills’ received the highest rating (90%) highlighting the necessity for cybersecurity professionals to clearly and effectively communicate complex security concepts, ensuring that program content resonates with diverse audiences. This was followed by ‘Adaptability and Continuous Learning’ (88%), demonstrating the dynamic nature of cybersecurity threats and the critical need for professionals to consistently update their knowledge and adjust training programs to emerging challenges. ‘Creative Thinking’ (86%) and ‘Collaboration and Teamwork’ (84%) were also recognized as essential, emphasizing the value placed on developing engaging training materials and the importance of effectively collaborating with other departments and professionals to ensure that awareness-raising and training programs are comprehensive, relatable to the organization’s environment, and impactful. ‘Empathy and Active Listening’ and ‘Project Management’ also attracted substantial attention (80%) indicating the importance professionals place both on understanding employee perspectives to enhance training relevance and effectiveness and on ensuring that SETA initiatives are systematically organized, well-executed, and aligned with organizational needs.

When combining the percentages of participants who rated transferable skills as ‘Moderately Important’, ‘Slightly Important’, or ‘Not Important at all’, a deeper insight emerges regarding skills perceived as somewhat less critical. Notably, ‘Talent Management’ showed the highest combined percentage (28%), indicating that a significant number of professionals view assessing and managing employee competencies as less directly critical in designing SETA programs. Similarly, ‘Networking Skills’ (28%), ‘Leadership’ (26%), and ‘Cultural Awareness and Sensitivity’ (24%) had relatively higher combined lower-importance ratings, suggesting that these skills, while beneficial, may be seen as complementary rather than central to SETA program development.

4.4. Educational Methods for Effective Cybersecurity Program Design

The exploration of cybersecurity experts’ insights pertinent to the most appropriate educational methods in the context of cybersecurity education is an important contribution of the current study. Participants were invited to assess the importance of educational methods for creating effective and engaging SETA programs (Figure 4).

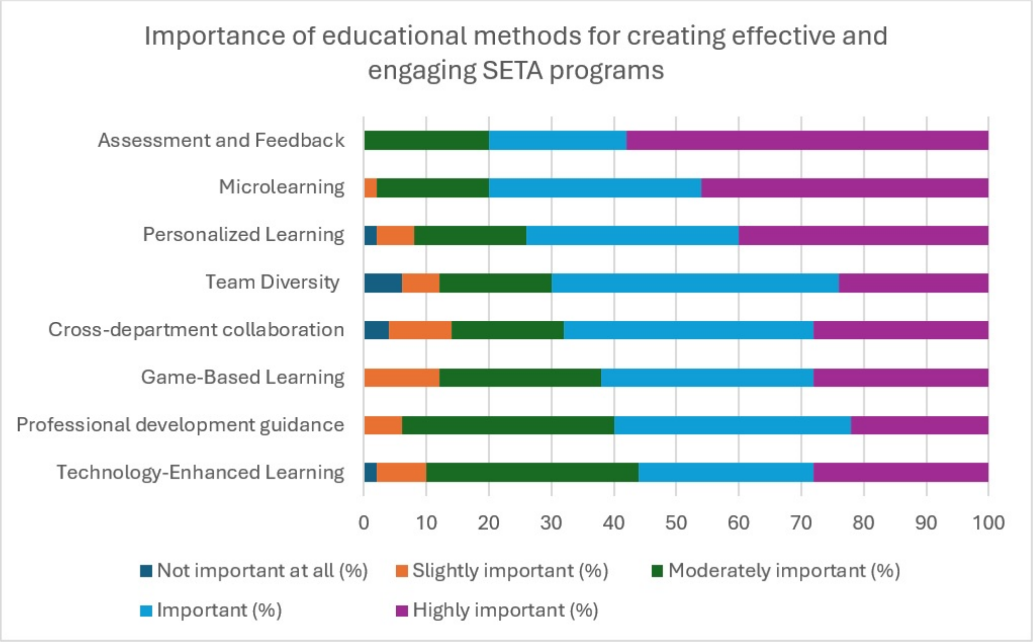


Figure 4: Professionals' Ratings of Educational Methods Essential for SETA Program Design (%) (Source: Authors own work)

The results highlight a clear preference among professionals for certain educational methods they consider particularly effective for the design of cybersecurity awareness and training programs. The top three methods voted as ‘Important’ to ‘Highly Important’ are: ‘Assessment and Feedback’ (80%), highlighting the critical role regular evaluation and immediate feedback play in educational effectiveness by enabling learners’ continuous improvement while also allowing customization of programs to address learners' evolving needs and skill gaps; ‘Microlearning’ (80%), indicating the importance professionals attribute to delivering learning content in smaller, manageable pieces, and 'Personalized Learning' (74%), recognizing that tailoring learning pathways to individual learners' strengths, needs, and interests makes learning more relatable and maximized impact for each learner. On the other hand, 'Professional Development Guidance', while important in integrating guiding elements in SETA programs and helping learners link training with long-term growth, it was not universally viewed as a top priority. This indicates that participants might prioritize direct training effectiveness over longer-term professional growth aspects. 'Cross-department Collaboration and 'Team Diversity' also elicited diverse responses. While many participants acknowledged their value, some ambiguity is evident about their direct impact on the effectiveness of SETA programs.

Other educational methods, while still recognized as valuable by at least 56% of the participants, received a higher (combined) percentage across the three lower-importance ratings. A surprising result was that 'Technology-enhanced Learning' was assigned a lower rating by most participants (44%) compared to all other educational methods, which may indicate that, while technology (e.g., AI-driven and other digital tools) can enhance engagement many learners may still prefer traditional or simpler approaches – even when the subject is a technology-oriented one like cybersecurity. Similarly, 'Game-based Learning', though known to be effective in boosting motivation and engagement, was rated with a lower combined importance rating (38%). These results highlight key pedagogical considerations since instructional designers need to ensure their programs are inclusive, relevant, and address the needs of diverse learners.

4.5. Importance of Team Composition and Experience

Participants' insights were also gathered on the importance of aspects related to team composition and experience when developing cybersecurity awareness-raising and training programs (Figure 5).

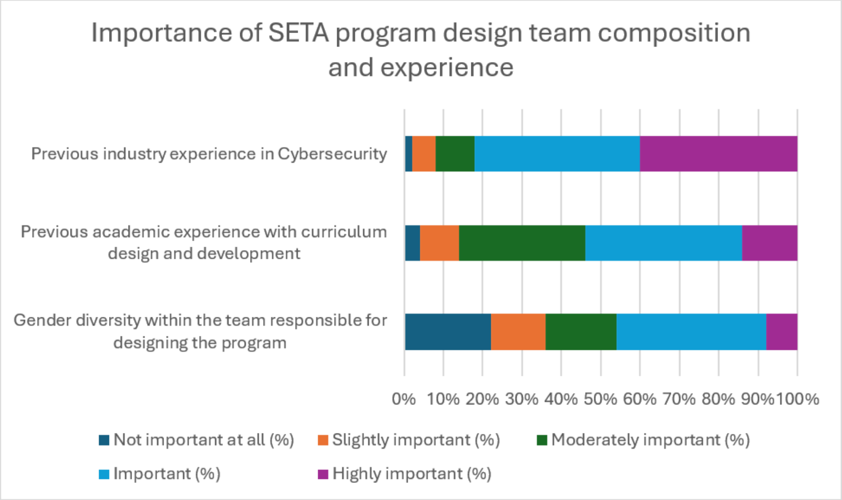
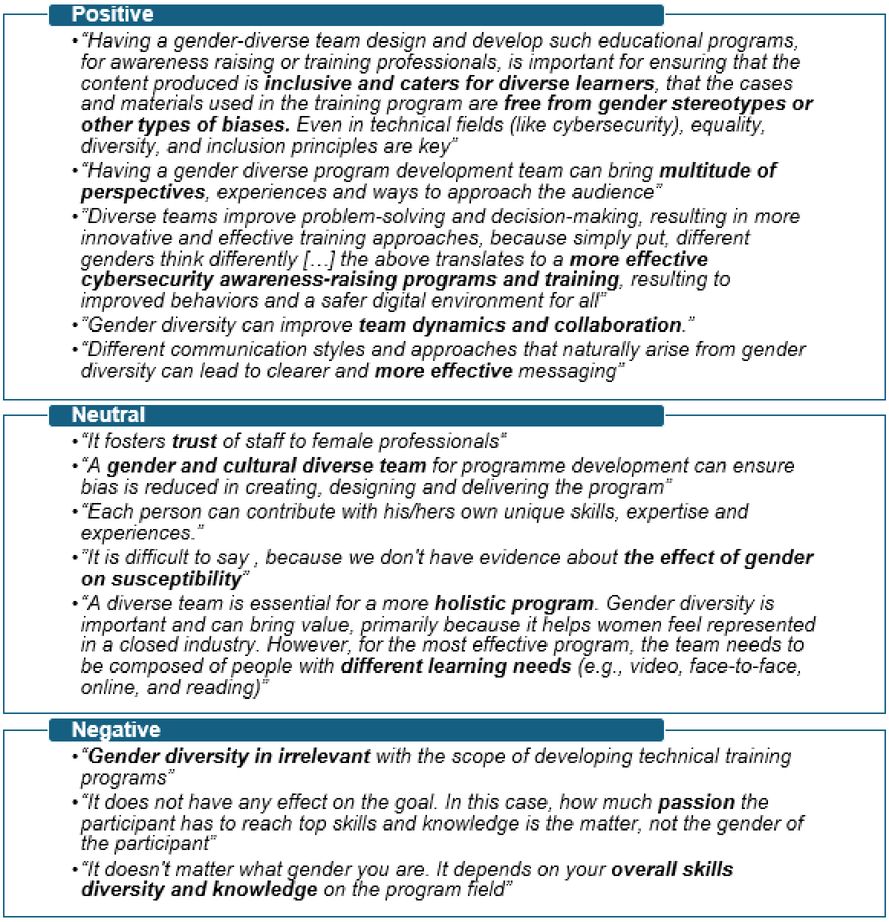


Figure 5: Professionals' Ratings of SETA Program Design Team Composition and Experience Importance (%) (Source: Authors own work)

'Previous Industry Experience in Cybersecurity' was identified as the most critical factor, with a combined 82% of respondents rating it as either 'Highly Important' or 'Important'. This indicates that practical, hands-on cybersecurity experience is highly valued and perceived as integral for effectively designing and delivering impactful cybersecurity education and training programs. 'Previous Academic Experience with curriculum design and development' received lower importance with a significant 42% considering it as either 'Slightly important' or 'Moderately important', suggesting that direct academic experience in curriculum development, while appreciated, may not be seen as essential if supplemented by strong practical industry knowledge.

The ratings received on 'Gender Diversity within cybersecurity program development teams' were notably more distributed across rating bands. Only 8% rated it as 'Highly Important' while a significant proportion of 22% rated it as 'Not Important at all'. The gender diversity aspect in SETA development teams was further investigated through an open-ended question where 41 respondents provided feedback regarding the perceived effectiveness gender-diverse development teams can bring into SETA program design. A sentiment analysis was performed on the responses to capture positive, neutral, or negative feelings regarding gender diversity. Figure 6 presents representative verbatim quotes from each cluster. Participants with positive sentiment (approximately 44%) explicitly acknowledged and supported the role of gender diversity, emphasizing several advantages. They particularly highlighted how gender-diverse teams contribute to more inclusive, comprehensive, and effective program designs. These respondents noted benefits such as broader and more diverse perspectives that foster creativity, innovation, and better problem-solving, improved program communication, better catering to diverse audiences and varied learning needs. Overall, respondents with positive sentiment clearly articulated the value of gender diversity, not merely as an ethical consideration but as a strategy for enhancing cybersecurity training effectiveness. Neutral respondents (approximately 27%) acknowledged gender diversity to varying degrees yet did not emphasize it as significantly impactful. These respondents generally indicated that gender diversity provides additional perspectives or helps avoid bias, but without deeply elaborating on specific advantages. It was observed that the emphasis was frequently placed on broader diversity (expertise, roles, background) rather than gender alone. Negative sentiment was also represented in a considerable portion of responses (29%). These participants eliminated the relevance of gender diversity in cybersecurity program development focusing simply on merit and expertise. It was emphasized that technical skills, individual competencies, passion, and knowledge are the primary drivers of effectiveness, rather than gender composition (Figure 6).



Positive

- “Having a gender-diverse team design and develop such educational programs, for awareness raising or training professionals, is important for ensuring that the content produced is **inclusive and caters for diverse learners**, that the cases and materials used in the training program are **free from gender stereotypes or other types of biases.** Even in technical fields (like cybersecurity), equality, diversity, and inclusion principles are key”
- “Having a gender diverse program development team can bring **multitude of perspectives**, experiences and ways to approach the audience”
- ”Diverse teams improve problem-solving and decision-making, resulting in more innovative and effective training approaches, because simply put, different genders think differently […] the above translates to a **more effective cybersecurity awareness-raising programs and training**, resulting to improved behaviors and a safer digital environment for all”
- ”Gender diversity can improve **team dynamics and collaboration**.”
- “Different communication styles and approaches that naturally arise from gender diversity can lead to clearer and **more effective** messaging”

Neutral

- “It fosters **trust** of staff to female professionals"
- “A **gender and cultural diverse team** for programme development can ensure bias is reduced in creating, designing and delivering the program”
- “Each person can contribute with his/hers own unique skills, expertise and experiences.”
- ”It is difficult to say , because we don't have evidence about **the effect of gender on susceptibility**”
- “A diverse team is essential for a more **holistic program**. Gender diversity is important and can bring value, primarily because it helps women feel represented in a closed industry. However, for the most effective program, the team needs to be composed of people with **different learning needs** (e.g., video, face-to-face, online, and reading)”

Negative

- “**Gender diversity in irrelevant** with the scope of developing technical training programs”
- “It does not have any effect on the goal. In this case, how much **passion** the participant has to reach top skills and knowledge is the matter, not the gender of the participant”
- “It doesn't matter what gender you are. It depends on your **overall skills diversity and knowledge** on the program field”

Figure 6: Sentiment analysis of participants’ perspectives on the role of gender-diverse teams (Source: Authors own work)

4.6. *Importance of cyber ranges role in the development of effective SETA programs*

Participants were asked to evaluate the importance of utilizing cyber ranges in the context of developing cybersecurity awareness-raising and specialized cybersecurity training programs (Figure 7). In the former case 78%

of professionals considered these as ‘Important’ or ‘Very important’, while in the latter case they unanimously agreed (100%) that cyber ranges are essential for effectively training professionals. Notably, 22% of participants perceived cyber ranges as ‘Somewhat Important’ or ‘Not Important’ for non-technical staff, indicating that cyber ranges usage might not be prioritized or perceived essential for general awareness-raising initiatives.

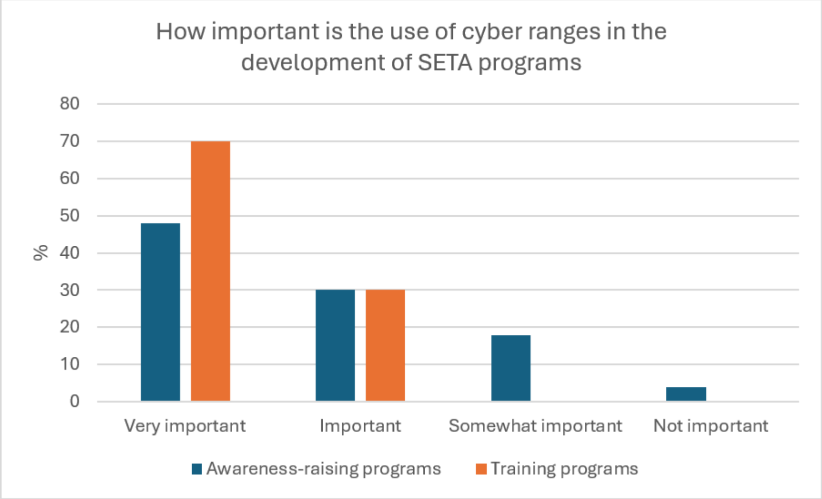


Figure 7. Professionals' ratings (%) of the use of cyber ranges in the development of effective SETA programs (Source: Authors own work)

4.7. ECSF Cybersecurity Career Roles Important for SETA Program Design

Participants were asked to select from the list of ENISA ECSF cybersecurity career roles all those they consider important to include in a team that will design (a) a cybersecurity awareness-raising program and (b) a cybersecurity training program (Figure 8). Responses revealed various insights into preferred roles for each type of program and highlighted notable similarities and differences.

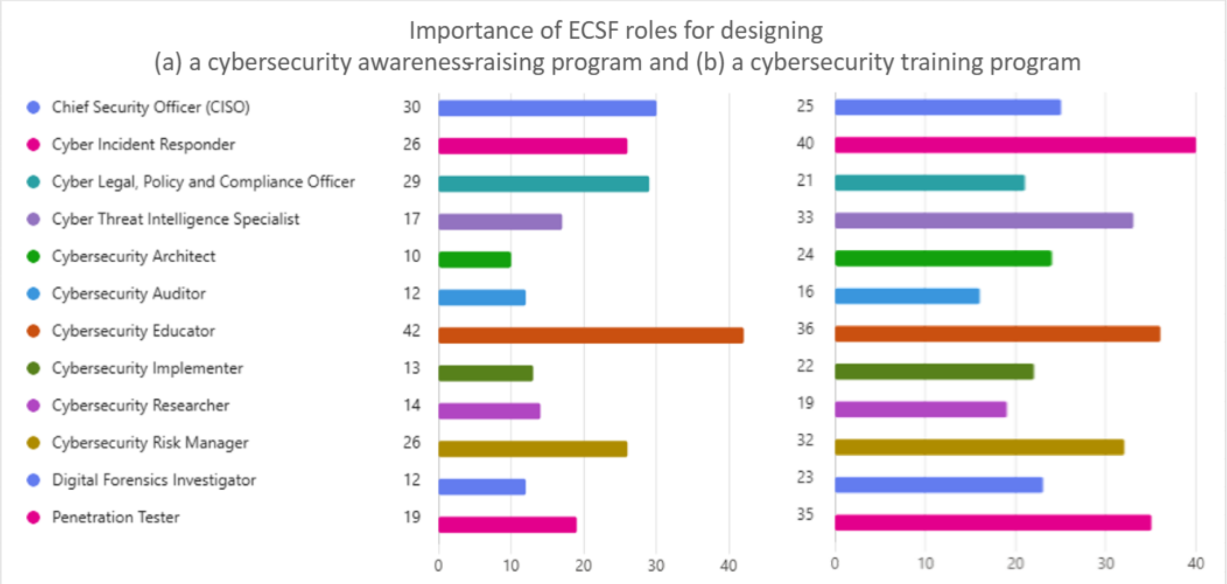


Figure 8. Importance of ECSF roles for designing (a) awareness-raising vs. (b) specialized training programs (Source: Authors own work)

A notable observation is that Cybersecurity Educator stands out as key role in both types of SETA programs and the most important for non-IT staff. The next most important roles for designing awareness-raising programs were Chief Information Officer (CISO) and Cyber Legal, Policy and Compliance Officer. Participants’ preferences highlight important aspects: the necessity for professionals specifically trained in instructional design, curriculum development, training delivery, and communication to effectively engage non-technical staff; the strategic oversight and authority needed to effectively position cybersecurity initiatives within organizational structures; and the importance of aligning awareness programs with organizational policies, regulations, and compliance requirements, respectively.

In terms of designing specialized training programs, the most prominently selected role was the Cyber Incident Responder reflecting a strong emphasis on real-world incident handling expertise, essential for advanced technical training. Cybersecurity Educator is consistently recognized as important and ranked second, confirming educators' roles in creating structured and effective learning experiences. Penetration tester is ranked third highlighting the technical expertise of this role as necessary for advanced technical skill development.

5. Discussion

5.1. Comparative Analysis of Knowledge Areas and Skills for Awareness-Raising vs. Specialized Training Programs

For awareness-raising programs, participants prioritized knowledge that supports practical understanding and behavior change among non-technical staff. High importance was given to topics like Cyber Threats, Data Protection, and Security Policies, reflecting a clear preference for content that communicates risks and promotes data protection practices. However, areas such as Incident Response and Management, Network Security Fundamentals, and Risk Management Principles were perceived as less critical for this audience, suggesting that highly technical or strategic concepts may not resonate as effectively in general awareness efforts. Such a perspective highlights the importance of carefully aligning program content with the audience's role-specific needs, reinforcing the notion that highly technical topics might need simplification or selective inclusion to maintain engagement and effectiveness in cybersecurity awareness programs.

In contrast, specialized training programs targeting IT professionals attracted a strong emphasis on technical depth and practical competencies. Participants rated topics like Incident Response and Management, Best Practices Using Security Tools and Technologies, and Network Security Fundamentals significantly higher for this audience. This reflects the expectation that cybersecurity professionals require advanced, hands-on training that equips them with the technical expertise needed to detect, analyze, and respond to complex threats. Interestingly, areas such as Security Frameworks and Standards, which received mixed ratings in awareness contexts, were seen as more critical in specialized training, likely due to their relevance to compliance and technical governance roles.

In terms of transferable skills, Communication Skills, Adaptability and Continuous Learning, and Creative Thinking were broadly recognized as essential across both program types. However, skills such as Leadership, Cultural Awareness and Sensitivity did not receive the same attention. This suggests that these skills, while beneficial, may be seen as complementary rather than central to SETA program development. Specifically, leadership, although important for motivating and guiding teams, may be viewed by some respondents as secondary in importance skills such as clear communication and adaptability. Additionally, cultural awareness and sensitivity might be considered less central due to a possible perception that cybersecurity training content is universally applicable regardless of cultural context, particularly in more technically oriented programs. A valuable future direction would be to explore the contextual impact of underemphasized transferable skills, such as Leadership and Cultural Awareness and Sensitivity, in the design and delivery of SETA programs. While these skills were not rated as central by many participants, further investigation could determine whether their contribution becomes more pronounced in certain organizational settings, such as multinational environments, culturally diverse teams, or programs requiring behavioral change at scale.

Overall, this comparative analysis reinforces a key insight, that SETA programs must be audience centric. Awareness programs should prioritize clarity, engagement, and behavioral change, while training programs must go deeper into technical mastery and operational readiness. Going forward, future SETA programs design should adopt differentiated instructional design strategies to ensure that each type of program delivers maximum relevance and impact to its intended audience.

5.2. Cybersecurity Roles Essential to SETA Program Development

The findings of this research reinforce the importance of adopting a multidisciplinary approach when assembling teams responsible for the development of SETA programs. For awareness-raising programs targeting non-IT staff, professionals identified the Cybersecurity Educator, CISO, and Cyber Legal, Policy, and Compliance Officer as critical roles. On the other hand, for specialized training programs aimed at IT professionals, roles like Cyber Incident Responder, Penetration Tester, and Cybersecurity Educator emerged as critical. Essential overlaps include the Cybersecurity Educator, emphasizing the crucial role of educational expertise. Differences highlight that technical roles such as Cyber Incident Responders and Penetration Testers become increasingly critical for specialized training. This can also reflect the training priorities as perceived by respondents and the importance of role-specific training design, where the depth and focus of content must align with the learners' existing expertise and professional responsibilities.

The combined insights from the current research and previous work (Charalambous and Stavrou, 2024) confirm that no single role can effectively carry the weight of SETA program development. A robust SETA development team should combine educational expertise, strategic oversight, and technical proficiency to enable the design of effective and sustainable cybersecurity education and training initiatives. A critical future direction, therefore, is to increase awareness within the cybersecurity domain regarding the benefits of formulating multidisciplinary SETA development teams. This could be supported through professional development opportunities, inclusion of SETA-related content in cybersecurity education pathways, and greater visibility of successful SETA programs developed through cross-functional collaboration. Additionally, as SETA programs evolve in complexity and scale, frameworks like the ECSF could be expanded to more explicitly capture and validate competencies related to awareness-raising and training programs' design, ranging from technical to soft skills such as leadership, empathy, and communication. Doing so would help formalize these often-overlooked dimensions of cybersecurity capability.

Ultimately, building a sustainable cybersecurity culture requires shifting professional mindsets, not only to broaden participation in SETA programs development but also to recognize that the effectiveness of cybersecurity education is not only about the content itself (what is being taught), but equally about how that content is communicated, taught, and experienced by learners. Empowering cybersecurity professionals to value and understand these aspects is key to achieving this shift.

5.3. The Role of Cyber Ranges in Cybersecurity Awareness-Raising and Training Programs

Cyber ranges have emerged as a powerful educational method for cybersecurity training (Floros *et al*, 2024), providing controlled and safe environments where participants can engage in realistic, hands-on scenarios. The findings of this research reveal a clear consensus among professionals regarding the value of cyber ranges, particularly in the context of specialized training programs for IT and cybersecurity professionals. In contrast, the role of cyber ranges in awareness-raising programs targeting non-technical staff was acknowledged with more varied perceptions. While a substantial portion of participants still recognized their value, there was a noticeable degree of caution, with some potentially viewing such environments as too complex or resource-intensive for general audiences. This disparity reflects an important distinction in how cyber ranges are currently perceived: as highly effective tools for skills-based, technical training, but requiring thoughtful adaptation for use in broader, non-specialist awareness initiatives.

Nonetheless, the potential of cyber ranges in awareness-raising programs should not be overlooked. When appropriately designed, cyber range activities can support experiential learning even for non-technical participants, particularly through simplified simulations, gamified experiences, or role-based exercises that contextualize common threats, such as phishing, or ransomware, in a tangible way. These experiential methods can reinforce key messages, foster behavioral change and empower learners to increase their confidence in applying best practices.

Future research should investigate how cyber range platforms can be adapted or scaled to suit various audience profiles, including employees with limited technical expertise. This includes exploring modular or tiered simulations that align with different learning goals and user capabilities. Additionally, evaluating the impact of cyber ranges on learning retention, engagement, and real-world readiness, across both technical and non-technical audiences, could provide critical insights and evidence into their broader applicability.

5.4. Effectiveness of Educational Methods in SETA Program Development

Findings revealed that certain educational methods, including ‘Assessment and Feedback’, ‘Microlearning’ and ‘Personalized Learning’, emerged as a central pillar for designing effective SETA programs. Regular feedback and assessment play a crucial role in tracking learning progress but also as a means of reinforcing knowledge retention and maintaining engagement over time (Godwin, 2025). The ability to provide learners with ongoing opportunities to reflect on their understanding and performance is essential in ensuring effective professional development. Another highly valued method was microlearning. By delivering content in smaller segments, SETA programs can enhance learners’ retention and can be more easily integrated into daily workflows without overwhelming the learner. This method can support the creation of more flexible and adaptive training experiences (Taherdoost, 2024) that are better suited to the diverse roles and time constraints of employees. Microlearning is also strongly linked to supporting personalized learning, which can adapt to learners’ strengths, needs, and interests. Personalized learning paths are essential in maintaining learner engagement (Taherdoost, 2024), ensuring that cybersecurity training resonates with diverse learning styles, preferences, and skill needs (Godwin, 2025), ultimately enhancing SETA program effectiveness. Rather than relying on a one-size-fits-all model, personalized SETA programs allow participants to focus on the areas most relevant to their needs and responsibilities.

An interesting contrast emerged between ‘Personalized Learning’ and ‘Professional Development Guidance’, two methods that share a common emphasis on tailoring SETA programs to individual needs and long-term growth. While personalized learning was widely regarded as a core method for SETA program effectiveness, professional development guidance was perceived as a more complementary rather than foundational element. This distinction suggests that participants prioritized immediate, learner-centric adaptability over broader career-oriented outcomes. This indicates that while both approaches support individual development, they are perceived to serve different layers of the learning experience: one immediate and practical, the other developmental and aspirational. Building on this distinction, future investigations could focus into how 'Personalized Learning’ and ‘Professional Development Guidance’ intersect and influence long-term cybersecurity culture development. One area worth exploring is whether integrating professional development elements into personalized learning pathways could strengthen learners' motivation and engagement, particularly among technical staff seeking to align training with career advancement (Kallonas *et al*., 2024).

The use of ‘Technology-enhanced Learning’, particularly through the integration of generative AI and other digital tools, was recognized by participants as having potential to support the creation of engaging and innovative cybersecurity learning experiences. However, the results also reveal a cautious stance among a notable portion of respondents, suggesting a level of uncertainty or reservation around its effectiveness or readiness for broad implementation within SETA programs. This reservation provides grounds for future research investigations. One key direction is to investigate the conditions under which technology-enhanced methods are most effective, for example, whether they are better suited for initial engagement, ongoing reinforcement, or personalized feedback.

Moreover, the low emphasis on ‘Cross-departmental Collaboration’ might reflect organizational silos during SETA program development. This might be due to the perception that cybersecurity training is primarily an IT concern, rather than an organization-wide initiative requiring active collaboration with other departments. Exploring how interdepartmental collaboration, particularly with HR, communications, and compliance units, affects the relevance, reach, and effectiveness of cybersecurity awareness and training programs could yield valuable insights. Future research could involve conducting comparative studies to assess whether programs designed by diverse teams result in greater learner engagement, improved behavior change, or higher knowledge retention.

Overall, these insights highlight the need for SETA programs to integrate well-defined feedback mechanisms, deliver short, targeted learning modules, and personalize the learning experience. On the other hand, methods like technology-enhanced and game-based learning, professional development guidance, cross-department collaboration, and team diversity should be strategically employed based on organizational context and specific audience characteristics, to optimize program relevance and impact.

5.5. Fostering Inclusive Approaches for Effective SETA Program Design

Findings underline professionals' clear prioritization of practical, industry-based cybersecurity experience in designing effective SETA programs. This aligns with the qualitative insights indicating that real-world cybersecurity experience significantly enhances program relevance and effectiveness. The moderate valuation of academic experience suggests that curriculum development aspects might not be evident to practitioners. This observation is further supported by an interesting observation made when comparing the strong support for including the Cybersecurity Educator role in SETA development teams with the more mixed perceptions regarding the value of previous academic experience in curriculum design and development. While many respondents recognized the importance of having an educator involved, likely due to their expertise in instructional methods and learning engagement, this did not seem to translate into a clear appreciation for academic or pedagogical experience more broadly. This suggests a potential disconnect: professionals may value the presence of an educational role in theory but may not fully associate this role with the formal expertise and methodologies typically gained through academic practice. It may also reflect a tendency to prioritize technical expertise and applied knowledge over theoretical or research-informed approaches. This finding highlights the need for greater awareness within the cybersecurity community of how educational science and instructional design can directly enhance the quality and impact of SETA programs. It also points to an opportunity to strengthen collaboration between cybersecurity practitioners and education specialists, bridging the gap between content knowledge and pedagogical effectiveness.

Moreover, investigations revealed varying perceptions regarding gender diversity's impact on cybersecurity program effectiveness. While a clear segment recognized significant benefits and advocated strongly for gender diversity's practical advantages, an almost equally sizable group either did not perceive gender as a relevant factor in cybersecurity training contexts or was neutral about its role. The varied perceptions signal an important area for further exploration and awareness-raising within cybersecurity professional communities. Looking ahead, the development of effective and inclusive SETA programs calls for a more intentional and structured embrace of interdisciplinary collaboration and professional diversity. As one of the respondents commented: "*When designing programs, one has to consider a variety of aspects such as how to engage participants, how to motivate them to change their behavior, how to connect with participants, what are the challenges they are facing, how the program can address these challenges, what topics should be included to make the program interesting, etc. A different set of skills is required to achieve the aforementioned, ranging from technical competency, emotional intelligence, self-direction, leadership skills, etc. Identifying the skills that each gender shows increased performance and then specify how this can be leveraged to design the programs will be highly beneficial*." Future programs should be designed by teams that bring together the practical insights of cybersecurity practitioners with the pedagogical expertise of educators who understand how people learn, retain, and apply knowledge. This synergy is particularly crucial for translating technical accuracy into engaging and impactful learning experiences, highlighting the need to shift from siloed design practices to co-creation approaches that reflect the complex and human-centered nature of cybersecurity education (Al-Nuaimi, 2024; Godwin, 2025).

5.6 Implications for practice

The findings of this research carry important implications for academia, industry, policymakers, and practitioners seeking to enhance the design, delivery, and impact of SETA programs. As cybersecurity threats continue to evolve it is important to redesign the educational approaches employed and develop effective SETA programs for cultivating a strong cybersecurity culture. This is an initiative that requires a holistic design, cross-disciplinary collaboration, and sustained organizational support.

In academic settings, these findings highlight the need for programs of study in cybersecurity to place greater emphasis on SETA as a strategic tool for developing organizational cybersecurity culture (Grill *et al.*, 2025; Tran *et al*., 2025). Curriculum design should move beyond theoretical discussions of awareness and training, and instead offer practical, experience-based learning interventions that help students understand how to design effective SETA programs (Stavrou and Furnell, 2025). Key topics should include audience analysis, instructional design principles, stakeholder collaboration, and the use of educational technologies such as cyber ranges and gamified learning tools. Furthermore, academic programs should explicitly aim to build appropriate competencies related to designing SETA programs, enabling future cybersecurity professionals to take active, informed roles in SETA development when entering the workforce. Equally important is the development of transferable skills such as communication, adaptability, and empathy, some of which are often underrepresented in technical curricula but are essential for designing engaging and impactful learning experiences. By embedding these skills within cybersecurity education, academia can better prepare graduates not only to defend systems but also to educate and influence organizational behavior in support of a security-first mindset.

For industry, the findings challenge organizations to move beyond viewing SETA as a compliance checkbox and recognize it as a strategic investment. Effective SETA development requires time, money, and human resources. These investments are necessary for building and sustaining a resilient cybersecurity culture. Organizations must acknowledge that SETA is not a one-person task. Rather, it demands a collaborative, cross-departmental effort, bringing together technical experts, legal advisors, educators, and other professionals to co-design content that is accurate, relevant, and engaging. Executive support and interdepartmental coordination are crucial for embedding cybersecurity values into daily organizational practices.

Policymakers also have a key role to play in guiding and supporting the development of effective SETA programs. Cybersecurity policies should include clear guidelines for SETA program design and implementation, including recommendations for team diversity, multidisciplinary collaboration, and the use of innovative educational strategies and tools such as cyber ranges, supporting scenario-based simulations. Additionally, policies should emphasize the importance of role-based training, differentiating between the needs of IT and non-IT staff, and ensuring that all employees are empowered to understand and respond to cyber risks relevant to their responsibilities.

Practitioners, cybersecurity trainers, and Higher Education curriculum developers, can use the insights from this research to inform their practices and further develop their competencies. Understanding the distinct skills and knowledge areas required for different types of SETA programs allows practitioners to better align their content and delivery methods with the specific needs of their audience. This can lead to more engaging, impactful programs that support both organizational objectives and workforce development.

Finally, skills frameworks such as the ENISA ECSF should be extended to reflect the requirements of SETA program design. One important recommendation is to explicitly differentiate between the roles and competencies required for awareness-raising versus specialized technical training. Such distinctions would provide clearer guidance to academic institutions developing curricula, organizations' building teams, and policymakers shaping future workforce strategies. By mapping SETA-related skills more explicitly within these frameworks, the cybersecurity community can build a stronger foundation for inclusive, effective, and sustainable education and training practices.

6. Conclusions

This research set out to explore the distinct knowledge areas and skills required for the effective redesign of cybersecurity awareness-raising and specialized training programs, expanding on the foundations established in the previous literature-oriented research (Charalambous and Stavrou, 2024). By distinguishing between the needs of learners with non-technical and technical backgrounds, and gathering insights from cybersecurity professionals, the study offers a clearer understanding of what it takes to design SETA programs that are not only informative but also engaging, inclusive, and impactful.

The findings reaffirm that awareness-raising and training programs serve fundamentally different purposes and must be tailored accordingly. Awareness programs for non-IT staff require a strong emphasis on behavioral change, practical relevance, and clear communication, while specialized training programs targeting cybersecurity professionals demand deeper technical competencies, hands-on practice, and alignment with role-specific responsibilities. Despite these differences, certain knowledge areas, such as cyber threats, data protection, and security policies, were commonly valued, reflecting a shared foundation of cybersecurity understanding across both audiences. Transferable skills such as communication, adaptability, and creative thinking were consistently identified as critical across both program types, further highlighting the human-centered nature of cybersecurity education. The study also reinforced the importance of adopting a multidisciplinary and diverse approach to SETA program development. The inclusion of roles such as the Cybersecurity Educator, CISO, and Incident Responder illustrates that no single role can shoulder the responsibility of program design. Instead, collaboration between professionals with technical, strategic, and educational expertise is essential to ensure that programs are accurate, pedagogically sound, and relevant to varied organizational needs. Finally, this research highlights emerging opportunities and challenges related to the integration of cyber ranges, which hold potential for increasing learner engagement and retention. Although the study's sample size and composition could limit generalizability, the results offer an insight into professionals' perspectives on key factors providing a foundation for rethinking how SETA programs are designed. Placing greater emphasis on targeted skillsets, audience-specific strategies, and collaborative development models are essential steps toward enhancing the overall effectiveness, relevance, and sustainability of cybersecurity awareness and training initiatives. These insights can offer valuable guidance for academia, industry, policymakers, and practitioners as they work together to shape the future of cybersecurity education and workforce development.

References

Al-Nuaimi, M.N. (2024), "Human and contextual factors influencing cyber-security in organizations, and implications for higher education institutions: a systematic review", *Global Knowledge, Memory and Communication*, Vol. 73 No. 1/2, pp. 1-23. https://doi.org/10.1108/GKMC-12-2021-0209

Alyami, A., Sammon, D., Neville, K. and Mahony, C. (2023), "The critical success factors for Security Education, Training and Awareness (SETA) program effectiveness: a lifecycle model", *Information Technology & People*, Vol. 36 No. 8, pp. 94-125. https://doi.org/10.1108/ITP-07-2022-0515

Alyami, A., Sammon, D., Neville, K. and Mahony, C. (2024), "Critical success factors for Security Education, Training and Awareness (SETA) programme effectiveness: an empirical comparison of practitioner perspectives", *Information and Computer Security*, Vol. 32 No. 1, pp. 53-73. https://doi.org/10.1108/ICS-08-2022-0133

Armas, R. and Taherdoost, H. (2025), "Building a Cybersecurity Culture in Higher Education: Proposing a Cybersecurity Awareness Paradigm". *Information*, Vol. 16 No. 5, p.336.

Braun, V. and Clarke, V. (2006), Using thematic analysis in psychology. *Qualitative Research in Psychology*, Vol. 3 No. 2, p.77-101.

Charalambous, A. and Stavrou, E. (2024), "Harnessing the Right Talent for SETA Programs: Cybersecurity Roles and Competencies that Make a Difference", in *International Symposium on Human Aspects of Information Security and Assurance (HAISA)*. Cham; Nature Switzerland: Springer, pp.130-144.

Chourasia, R. (2025), "AI-Enhanced Cybersecurity Training: Learning Analytics in Action", *International Journal of Advanced Research in Science, Communication and Technology*, pp.566-573.

Creswell, J. W., & Creswell, J. D. (2018), *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th ed.). SAGE Publications.

ENISA (2022), European Cybersecurity Skills Framework (ECSF) Role Profiles, available at: https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles (accessed 28 February 2025).

Floros, E., Stavrou, E., Smyrlis, M., Nikoloudakis, N., Potamos, G., Apostolidis, A., Bempis, P., Grigoriadis, A., Magkos, K., Merkouris, D., Spanoudakis, G., Stavrou, S., Trikos, S., Papadakis, S.E. (2025), "Towards the Design of Cyber Range Training Programs for Enhanced Preparedness, Investigating the Training Needs in Critical

Infrastructures", paper presented at *IEEE Global Engineering Education Conference (IEEE EDUCON 2025)*, 22-25 April, London, UK.

Godwin, Z.I. (2025), "How Human-Centered Cybersecurity (HCC) Training Fosters Organizational Cybersecurity Cultures (CSC)". In *Integrating Artificial Intelligence in Cybersecurity and Forensic Practices,* pp. 187-204, IGI Global Scientific Publishing.

Grill, M., Sommestad, T., Karlzén, H. and Pousette, A. (2025), "Training for improved information security culture: a longitudinal randomized controlled trial", *Information and Computer Security*, https://doi.org/10.1108/ICS-08-2024-0189

Goodman, L. A. (1961), Snowball sampling. *Annals of Mathematical Statistics*, Vol. 32 No. 1, p.148-170.

Gundu, T. (2024), "Learn, unlearn and relearn: adaptive cybersecurity culture model", in *International Conference on Cyber Warfare and Security,* pp. 95-102, Academic Conferences International Limited.

Hu, S., Hsu, C. and Zhou, Z. (2021), "The impact of SETA event attributes on employees' security-related Intentions: An event system theory perspective", *Computers & Security*, Vol.109, p.102404.

Hu, S., Hsu, C. and Zhou, Z. (2022), "Security education, training, and awareness programs: Literature review", *Journal of Computer Information* Systems, Vol. 62 No. 4, pp.752-764.

Kallonas, C., Piki, A., and Stavrou, E. (2024), "Empowering Professionals: A Generative AI Approach to Personalized Cybersecurity Learning", *IEEE Global Engineering Education Conference (EDUCON 2024)*, Kos, Greece, pp. 1-10, https://doi.org/10.1109/EDUCON60312.2024.10578894.

Kandpal, V., Ozili, P.K., Jeyanthi, P.M., Ranjan, D. and Chandra, D. (2025), "Cybersecurity and Ensuring Privacy in Digital Finance", *Digital Finance and Metaverse in Banking,* Emerald Publishing Limited, pp. 157-170. https://doi.org/10.1108/978-1-83662-088-420251007

Karimnia, R., Maennel, K. and Shahin, M. (2022), "Culturally-sensitive cybersecurity awareness program design for Iranian high-school students", *8th International Conference on Information Systems Security and Privacy (ICISSP)*.

Kirova, D. and Baumöl, U. (2018), "Factors that Affect the Success of Security Education, Training, and Awareness Programs: A Literature Review", *Journal of Information Technology Theory and Application (JITTA)*, Vol. 19 No. 4.

Pawar, S. and Palivela, H. (2025), "Need of Paradigm Shift in Cybersecurity Implementation for Small and Medium Enterprises (SMEs)", *International Journal of Cybersecurity Intelligence & Cybercrime*, Vol. 8 No. 1, p.4.

Piki, A., Stavrou, E., Procopiou, A., Demosthenous, A. (2023), "Fostering Cybersecurity Awareness and Skills Development Through Digital Game-Based Learning", in *10th International Conference on Behavioural and Social Computing (BESC)*, 30 October-1 November 2023, Larnaca, Cyprus.

Raj, R., Singh, A., Kumar, V. and Verma, P. (2024), "Achieving professional qualifications using micro-credentials: a case of small packages and big challenges in higher education", *International Journal of Educational Management,* Vol. 38 No. 4, pp. 916-947. https://doi.org/10.1108/IJEM-01-2023-0028

Shillair, R., Esteve-González, P., Dutton, W.H., Creese, S., Nagyfejeo, E. and von Solms, B. (2022), "Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise", *Computers & Security*, Vol. 119, p.102756.

Stavrou, E. and Furnell S. (2025), "What's in a Name? How Cyber Security Masters Degrees Compare", paper presented at *IEEE Global Engineering Education Conference (IEEE EDUCON 2025)*, 22-25 April, London, UK.

Stavrou, E. and Piki, A. (2024), "Cultivating self-efficacy to empower professionals' re-up skilling in cybersecurity", *Information & Computer Security*, Vol. 32 No. 4, pp. 523-541. https://doi.org/10.1108/ICS-02-2024-0038

Taherdoost, H. (2024), "Towards an Innovative Model for Cybersecurity Awareness Training". *Information*, Vol. 15 No. 9, p.512.

Tran, D.V., Nguyen, P.V., Le, L.P. and Nguyen, S.T.N. (2025), “From awareness to behaviour: understanding cybersecurity compliance in Vietnam”, *International Journal of Organizational Analysis*, Vol. 33 No. 1, pp. 209-229. https://doi.org/10.1108/IJOA-12-2023-4147

Trend Micro (2024), “Calibrating Expansion – 2023 Annual Cybersecurity Report”, available at: https://documents.trendmicro.com/images/TEx/articles/Calibrating_Expansion_2023_Annual_Cybersecurity_Report.pdf (accessed 28 February 2025).

Uchendu, B., Nurse, R.C., Bada, M., Furnell, S. (2021), “Developing a cyber security culture: Current practices and future needs”, *Computers & Security*, Vol. 109.

WEF (2025), World Economic Forum (WEF) Jobs of the Future Report, *Weforum.org*, available at: https://reports.weforum.org/docs/WEF_Future_of_Jobs_Report_2025.pdf (accessed 30 March 2025).