






Transforming threats into opportunities: The role of human factors in enhancing cybersecurity

Silvia Colabianchi ^a, Francesco Costantino ^{a,*}, Fabio Nonino ^a, Giulia Palombi ^b

^a Department of Computer, Control, and Management Engineering "Antonio Ruberti", Sapienza University of Rome, Via Ariosto 25, Rome 00185, Italy

^b Department of Engineering and Science, Universitas Mercatorum, Piazza Mattei, 10, Rome 00186, Italy

ARTICLE INFO

JEL classification:

000
039
033

Keywords:

Cyber resilience
Cyber-attack
Information security management
Digitalization
Socio-technical system
The Delphi study

ABSTRACT

In today's fast-paced digital landscape, the importance of human factors in cybersecurity has become increasingly evident yet is often overlooked. This research employs the Delphi method to achieve expert consensus on the managerial actions that enhance cybersecurity by leveraging human factors. The study offers 16 key managerial actions, highlighting the shift from viewing humans as sources of vulnerability to acknowledging them as essential components of cybersecurity solutions. The findings suggest developing an organizational culture that values cybersecurity, delineating clear roles and responsibilities, and fostering continuous learning. This approach emphasizes the importance for organizations to recalibrate their cybersecurity strategies and provides a roadmap for implementing the suggested managerial actions. The study contributes to the socio-technical debate with a particular focus on human factors and provides practical guidance for organizations to improve their future cybersecurity posture.

Introduction

In today's hyper-connected environment, there has been a remarkable increase in productivity, efficiency, and system integration, ushering in a new era of digital evolution. However, this unprecedented connectivity has also introduced several potential risks (Corallo et al., 2020). Rapid digital transformation has made organizations highly dependent on data and information within their integrated systems, opening the door to new risk scenarios (Buck et al., 2023; Carroll et al., 2023). This dependency amplifies the impact of cyber threats, putting business continuity, confidentiality, and reputation at risk.

The latest European Digital SME Report reveals a significant escalation in ransomware attacks in 2023 and highlights the publication of 7772 new potential issues in the Common Vulnerabilities and Exposures (CVE) database, further illustrating the dynamic and ever-changing nature of cyber vulnerabilities (European Digital, 2023). Mitnick and Simon (2003) noted that humans have become the most vulnerable aspect of systems. This statement remains relevant today due to the prevalence of cyber incidents driven by human involvement. According to Verizon's 2023 Data Breaches Investigations Report (Verizon, 2023), 72 % of data breaches involved a human element, including incidents related to social engineering attacks, errors, and misuse. IBM's 2023

Cost of a Data Breach Report (Cost of a data breach Report, 2023) identified human error as the cause of the most expensive forms of data breaches. The available data show a significant increase in incidents caused by inattention as the primary factor. In many cases, however, attributing incidents merely to oversight fails to fully capture the situation, because such incidents are often the result of a combination of human characteristics, workplace conditions (Donalds & Osei-Bryson, 2020; Neigel et al., 2020), and skill gaps (Aljohani et al., 2022). For years, organizations have relied on highly technical approaches that have only marginally considered human integration in their cybersecurity strategies. Investigations following numerous cyber incidents have consistently pointed to human error or negligence, identifying users as the weak link in establishing secure environments, with limited consideration given to end users' cognitive characteristics, needs, and motivations (Abzakh & Althunibat, 2023).

In this context, there is a growing interest in addressing the human aspects of cybersecurity by fostering an informed and proactive workforce (Zimmermann & Renaud, 2019). The field of study of human factors is defined as the "scientific discipline concerned with the understanding of the interactions among humans and elements of a system" (Bridger, 2018). As key aspects of cybersecurity, human factors are attracting increasing interest in this domain, due to their potential to

* Corresponding author.

E-mail address: francesco.costantino@uniroma1.it (F. Costantino).

<https://doi.org/10.1016/j.jik.2025.100695>

Received 16 September 2024; Accepted 12 March 2025

Available online 17 April 2025

2444-569X/© 2025 The Authors. Published by Elsevier España, S.L.U. on behalf of Journal of Innovation & Knowledge. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

frame humans as either a problem or a key part of the solution for cybersecurity (Desolda et al., 2021a). This focus has moved beyond a purely technological perspective, embracing a human-centric cybersecurity approach that prioritizes the design of security systems around user needs and behaviors while enhancing usability and reducing cognitive load (Warkentin et al., 2016). Additionally, through the socio-technical systems perspective, the technological aspects have been integrated with the social ones, enabling the analysis of the social, environmental, and technical aspects of cybersecurity and offering a multidimensional viewpoint (Malatji et al., 2019).

The intersection of human factors in cybersecurity and behavioral security theory offers valuable insights for mitigating risks by taking human behavior into account, ultimately improving overall security outcomes (Balozian et al., 2023; Chowdhury et al., 2019; Corradini, 2020a; Crossler et al., 2013; Donalds & Osei-Bryson, 2020; McIlwraith, 2021). Human factors also relate to human-computer interaction theory, which focuses on designing intuitive systems to enhance usability and reduce user errors by creating user-friendly security tools that fit seamlessly into workflows (Norman, 2017). The need to address the individual, organizational, and technological challenges posed by human factors in cybersecurity, as identified by Pollini et al. (2022), along with the recognition of human factors as key to unlocking the human potential in cybersecurity (Desolda et al., 2021a; Zimmermann & Renaud, 2019), underscores the importance of implementing managerial actions to increase cybersecurity. The objective of the study is to identify those managerial actions that enhance cybersecurity by leveraging the role of human factors. Accordingly, the study presents three main contributions. First, it compiles a set of managerial actions that leverage human factors in cybersecurity based on the existing literature. Second, it uses the Delphi method to reach a consensus on the key actions to undertake. Third, the actions that organizations should implement in the future have been ranked and prioritized with the guidance of experts, who recommended tools and best practices that should be adopted to enhance the potential of these managerial actions.

The remainder of the paper is organized as follows. Section "Background" provides an analysis of the theoretical background on managerial actions. In Section "Research design", the research design and methodological approach of a Delphi study are described. Section "Results" presents the results and the experts' perceptions regarding the future role of humans in cybersecurity management. Section "Discussion" discusses the contributions of the study. Section "Conclusions and future steps" concludes and offers ideas for future research.

Background

Human factors in cybersecurity

The field of human factors aims to enhance the interaction between individuals and technology. Extensive exploration of human factors has occurred in diverse fields, notably in health and aviation (Wiegmann & Shappell, 2017), with the aviation sector introducing notable frameworks such as "The Dirty Dozen," proposed by Dupont in 2009 (Dupont, 2009; Wiegmann & Shappell, 2017) and subsequently adopted in other fields such as healthcare (Poller et al., 2020), and cybersecurity (Desolda et al., 2021b).

Focusing on human factors in cybersecurity research, various classifications, ontologies, or simple reflections on which aspects of human character most influence cybersecurity have been proposed over the years. Specifically, a characterization of human factors, including human behavior, is necessary to understand how the actions of users, defenders (IT personnel), and attackers affect cybersecurity risk. A significant contribution comes from Oltramari et al. (2015), who presented the Human Factors Ontology (HUFO) focusing on trust. HUFO categorizes risk characteristics related to human factors, categorizing them into attackers, defenders, and users interacting with computer networks. The goal is to provide a tool for risk assessment and prioritization in

cyber operations. In another comprehensive work (Desolda et al., 2021b), the authors conducted a systematic review of the key research on human factors and phishing. They used the well-known Dupont factors as classification categories and describe the misbehavior of individuals concerning phishing phenomena. Another contribution (Gratian et al., 2018) examined how risk-taking preferences, decision-making styles, demographics, and personality traits all influence individual security behaviors regarding securing devices, creating passwords, proactive awareness, and updating.

Finally, an interesting paper by the Chartered Institute of Ergonomics and Human Factors (CIEHF, 2022) compiled a list of risky human behaviors and correlates them with cybersecurity issues and vulnerabilities.

Other contributions have examined the correlation between human characteristics and cybersecurity behavioral intentions, as well as their impact on compliance with cybersecurity procedures. These studies have focused on specific personality traits or types of attacks, such as social engineering. For example, Williams et al. (2018) investigated employees' susceptibility to phishing attacks and their responses to emails emphasizing authority and urgency. Similarly, Uebelacker and Quiel (2014) examined the role of the big five personality traits in susceptibility to social engineering. Finally, to provide a holistic method of measuring information security awareness, Parsons et al. (2017) developed the HAIS-Q questionnaire, a 63-item instrument assessing seven focus areas, each divided into knowledge, attitude, and behavior. Recently, Pollini et al. (2022) presented a holistic approach integrating the HAIS-Q model by classifying human factors into individual, organizational, and technological. They applied this framework to pilot healthcare organizations to analyze how HF vulnerabilities may impact cybersecurity risks (Bridger, 2018). Human factors in cybersecurity are analyzed from two main perspectives: the human-centric cybersecurity perspective and the socio-technical systems perspective. The human-centric cybersecurity approach places the user at the center of security design and practices (Pawlicka et al., 2022). This concept emphasizes understanding user needs, behaviors, and experiences to create security measures that are not only effective but also user-friendly. By focusing on the human element, organizations can develop systems that encourage secure behaviors and reduce users' cognitive load (Pinzone et al., 2020). This approach recognizes that technology alone cannot solve cybersecurity challenges. Instead, a deep understanding of human behavior is essential for crafting solutions that engage users and promote active participation in security practices (Warkentin et al., 2016).

Socio-technical systems theory offers a holistic framework for understanding the interplay between social and technical elements in organizations. This approach has led to the conceptualization of cyber socio-technical systems (Colabianchi et al., 2021; Patriarca et al., 2021) and a risk assessment framework that considers individual, organizational, and technological challenges posed by human factors in cybersecurity (Pollini et al., 2022). It argues that effective cybersecurity depends not only on technology but also on the human and organizational context in which these systems function. This theory emphasizes the need for collaborative efforts among technical teams, management, and users to create effective security solutions (Checkland & Scholes, 1999). By acknowledging the complex interactions between people, processes, and technology, socio-technical systems theory enriches the understanding of human factors in cybersecurity. It promoted a comprehensive approach to designing security systems that accommodate human behavior while addressing technical vulnerabilities (Malatji et al., 2019).

Several theories, including behavioral security and human-computer interaction theories, are crucial for understanding human factors. The behavioral security theory explores psychological and social influences on individuals' security-related behaviors. It aims to identify the motivations, attitudes, and decision-making processes that drive user behavior in cybersecurity contexts. For example, risk perception and social norms affect how individuals respond to security measures

Table 1**Managerial actions.**

Managerial actions description	Human Factors involved	Refs.
A1. Encouraging personal responsibility This action addresses the tendency of individuals to feel insecure and avoid engaging in cybersecurity procedures. Individuals often rely on devices or people, mistakenly believing that these are the sole responsible for system security. Increasing awareness of individual responsibility in cybersecurity is critical to promoting a proactive approach to protecting corporate data and systems.	Complacency; Knowledge	(Fard Bahreini et al., 2023; Henshel et al., 2015; Nwankpa & Datta, 2023)
A2. Reducing cognitive fatigue: Cognitive fatigue represents the maximum number of cognitive resources an individual can devote to security issues. Multiple policies and procedures can cause fatigue in employees who may feel stressed and exhausted due to excessive pressure and oversight in the workplace. Cognitive fatigue and associated cyber risks can be mitigated by properly balancing the number of norms when they are brought to the attention of employees (e.g., password changes).	Fatigue; Norms; Pressure; Resource; Stress	(Chowdhury et al., 2022; Corradini, 2020a; D'Arcy et al., 2009; Majumdar & Ramteke, 2022; Nobles, 2022; Nthala & Flechais, 2017; Reeves et al., 2023; Wang et al., 2012; Zimmermann & Renaud, 2019)
A3. Workload balance: The importance of workload management and effective scheduling of activities is emphasized to improve organizational cybersecurity. In situations of high mental stress or intense workload, employees are more likely to make mistakes due to distraction. Therefore, it is essential to balance workloads and plan activities wisely to ensure a more secure organizational environment.	Distraction; Fatigue; Pressure; Resource; Stress	(Chowdhury et al., 2022; Dekker & Hollnagel, 2004; Nobles, 2022; Nthala & Flechais, 2017; Wang et al., 2012)
A4. Adopting models and standards: The adoption and sharing of certain tools, such as recognized cybersecurity management frameworks and standards, will enable the organization to guide and manage its resources.	Resource	(Sarker, 2023; Taherdoost, 2022; Zimmermann & Renaud, 2019)
A5. Awareness campaigns: Awareness campaigns contribute to effective cybersecurity by making people aware of the risks involved. In addition, these campaigns explain the rationale behind the policies, procedures, and practices in place. They may include informational materials, workshops, and specialized training.	Awareness; Norms	(Mailloux et al., 2019; Wong et al., 2022; Young et al., 2018)
A6. Cybersecurity training: Training increases knowledge for more effective cybersecurity. Employees, when trained, can be the main driver of more effective cybersecurity. Innovative approaches to training (e.g., VR, games, chatbots) were found to be slightly more effective in raising cybersecurity awareness.	Communication; Knowledge; Norms	(Aker et al., 2022; Kruger & Kearney, 2006; Mailloux et al., 2019; McIlwraith, 2021; Olivares Rojas et al., 2022; Triplett, 2022)
A7. Dedicating staff to cybersecurity training: Most organizations suffer from a lack of staff dedicated to cybersecurity awareness programs. Resources responsible for awareness programs are often involved in other activities and areas, which limits their ability to fully commit to employee training.	Awareness; Resource	(Alahmari & Duncan, 2020; Chowdhury et al., 2019; Kompaso & Sridevi, 2010)
A8. Defining roles and responsibilities: It is essential to define the roles and responsibilities of each employee, regardless of their areas of expertise, in cybersecurity plans and policies. This process includes the assignment and explanation of the required tasks, functions, and activities.	Communication	(Yukl, 2013)
A9. Developing a cybersecurity-oriented culture: Developing a cybersecurity-oriented organizational culture involves the sharing of strategic goals and the communication of cybersecurity standards by linking them to corporate strategy.	Awareness; Communication; Knowledge; Teamwork	(Röcker, 2012)
A10. Encouraging feedback and peer learning: In the context of cybersecurity, fostering a culture of feedback and peer learning is critical to creating a secure business environment. This exchange of mutual assessments can help to quickly address a cyber threat and establish a culture of security awareness among all employees.	Awareness; Communication; Knowledge; Teamwork	(Kompaso & Sridevi, 2010)
A11. Scheduling cybersecurity activities: Organizations that adopt multiple IT applications and devices do not often include specific cybersecurity training associated with them. Scheduling time for this activity will make the use of these devices more effective and secure.	Knowledge	(European Union Agency for Network and Information Security, 2018)
A12. Sharing success stories: The term "success stories" identifies those events where cybersecurity information sharing has made a significant difference. These include situations where participants prevented harm by sharing incident reports and information on previous attacks. Promoting and communicating such "success stories" means recognizing those employees who identify potential attacks and/or report them to colleagues.	Awareness; Communication; Knowledge	(NIST, 2018)
A13. Simplifying procedures: Security policies and procedures are often filled with technical language and information that can be difficult to understand. This	Pressure; Stress	(D'Arcy et al., 2009; Gale et al., 2022; Proudfoot et al., 2024)

(continued on next page)

Table 1 (continued)

Managerial actions description	Human Factors involved	Refs.
complexity requires employees to invest time and effort into becoming familiar with these policies. Simplified communication of these procedures by the organization may reduce the burden on employees and improve the effectiveness of the policies themselves.		
A14. Team-level cybersecurity management: Aligning cybersecurity objectives at team level is crucial. A stronger team culture is suggested, where cybersecurity-related Key Performance Indicators (KPIs) are defined, incidents and difficulties communicated and cybersecurity is integrated into daily team activities.	Assertiveness; Communication; Knowledge; Stress; Teamwork	(Bao et al., 2016 ; Bassanino et al., 2014 ; Cavanaugh et al., 2000 ; Kompaso & Sridevi, 2010 ; Pinzone et al., 2020 ; Rogers & Ashforth, 2017 ; Zimmermann & Renaud, 2019)
A15. Adequacy of technical resources: It is essential that the organization takes responsibility for ensuring that staff have access to all the information, financial and material resources needed to do their jobs. In the context of cybersecurity, this includes maintaining all systems to ensure effective defense against cyber-attacks. The availability of adequate technical resources and their proper allocation and maintenance are critical to enabling individuals to maintain a sound cybersecurity posture.	Resource	(Alahmari & Duncan, 2020 ; Chowdhury et al., 2019 ; Kompaso & Sridevi, 2010 ; Zarreh et al., 2019)
A16. Incident reporting: An organization's cybersecurity can be significantly improved by changing the perspective on incident reporting, viewing it as a virtuous act rather than a source of shame for causing the incident. Creating an environment where incident reporting is encouraged and treated confidentially can help identify and mitigate vulnerabilities, thereby protecting the organization from potentially greater harm.	Communication; Teamwork	(Kompaso & Sridevi, 2010)
A17. Remote work cybersecurity: The proliferation of remote working requires organizations to rethink their training programs. In particular, companies need to supplement cybersecurity training with procedures specific to remote work.	Distraction	(Bergefurt et al., 2021 ; Miarmi & DeBono, 2007)
A18. Simulation of cyber incidents: People's lack of attention to cyber threats is often due to a lack of direct experience of significant cyber incidents that have disrupted critical services. A training process that provides employees with direct experience or that simulates a cyber-attack may improve skills and raise awareness.	Awareness; Complacency; Knowledge	(Akte et al., 2022 ; Frey, 2018 ; Jalali et al., 2019 ; Maalem Lahcen et al., 2020)
A19. Understanding the limitations of cybersecurity devices: A lack of understanding of cybersecurity devices leads individuals to overestimate the effectiveness of these devices in providing complete protection and to overlook the need for human oversight. Improving the understanding of such devices will contribute to more effective cybersecurity management and active oversight.	Distraction; Complacency; Knowledge	(Fard Bahreini et al., 2023 ; Henshel et al., 2015 ; Nwankpa & Datta, 2023)

([Herath & Rao, 2009](#)). By applying insights from behavioral security theory, organizations can develop targeted interventions that encourage positive security behaviors, such as adherence to password policies or timely reporting of phishing attempts. This understanding is critical to fostering a culture of proactive security within organizations ([Corradini, 2020b](#)).

Human-computer interaction theory examines how people interact with computers and technology. It focuses on designing interfaces that enhance usability and user experience. In cybersecurity, human-computer interaction principles can guide the creation of intuitive security systems that reduce user error and improve compliance with security protocols ([Carroll, 1997](#)). Effective human-computer interaction design considers factors such as cognitive load, user feedback, and the overall user journey, ensuring that security measures are seamlessly integrated into users' workflows ([Norman, 2017](#)).

Managerial actions to improve cybersecurity by enabling the positive role of human factors

According to the above-mentioned theories, the role of human factors in cybersecurity can be either negative or positive, depending on various aspects. Based on a combination of knowledge, attitude, and behavior ([Parsons et al., 2017](#)), people can either pose a threat or contribute to cybersecurity solutions ([Desolda et al., 2021b](#); [Ferro et al., 2022](#)). Several actions have been identified in the literature to ensure that human factors play a positive role in enhancing the cybersecurity of the organization. To provide a complete understanding of these managerial actions, current research on the influence of human factors in

cybersecurity, as well as sources describing the impact of one of the "The Dirty Dozen" human factors (i.e., Lack of Communication, Complacency, Lack of Knowledge, Distraction, Fatigue, Lack of Resources, Pressure, Lack of Assertiveness, Stress, Lack of Awareness, Norms) on cybersecurity were analyzed.

Initially, a general search was conducted using the broad terms (1) "human factors" and "cybersecurity," and (2) "human error" and "cybersecurity." We then refined our search by individually combining Dupont's factors with the term "cybersecurity" (e.g., "communication" and "cybersecurity" or "complacency" and "cybersecurity"). The bibliographical references provided are not exhaustive but rather serve as a starting point for the Delphi study, establishing a link between human factors and cybersecurity issues. The literature identified actions that can mitigate or improve certain human factors, ultimately benefiting cybersecurity. Table 1 presents the intervention actions, their descriptions, linked human factors, and references. When considering the Dupont human factors, the following actions have been identified:

- "Encouraging personal responsibility" can mitigate Complacency by increasing Knowledge;
- "Reducing cognitive fatigue" can mitigate Fatigue, Pressure, and Stress, and allow better usage of Resources and Norms;
- "Workload balance" can help reduce Distraction, Fatigue, Pressure, and Stress, and ensure better allocation of Resources;
- "Adopting models and standards" can allow better organizational Resource management;
- "Awareness campaigns" can increase the level of Awareness and the understanding of Norms;

- “Cybersecurity training” can increase Knowledge, Communication, and the understanding of Norms;
- “Dedicating staff to cybersecurity training” can raise Awareness and allow better Resource allocation;
- “Defining roles and responsibilities” can have a critical role in Communication;
- “Developing a cybersecurity-oriented culture” can improve Communication, Knowledge, Teamwork, and Awareness;
- “Encouraging feedback and peer learning” can improve Communication, Knowledge, Teamwork, and Awareness;
- “Scheduling cybersecurity activities” can increase Knowledge;
- “Sharing success stories” can have a positive effect on Communication, Awareness, and Knowledge;
- “Simplifying procedures” may result in working with a lower level of Pressure and Stress;
- “Team-level cybersecurity management” can have a positive effect on many factors including Communication, Knowledge, Teamwork, Stress, and Assertiveness;
- “Adequacy of technical resources” can improve the management of all the organizational Resources;
- “Incident reporting” can improve Communication and Teamwork;
- “Remote work cybersecurity” can mitigate Distraction;
- “Simulation of cyber incidents” can mitigate Complacency by increasing Knowledge and Awareness;
- “Understanding the limitations of cybersecurity devices” can mitigate Distraction and Complacency by increasing Knowledge.

Research design

The Delphi approach was employed to validate the managerial actions needed to enhance the human role in cybersecurity management and to prioritize them based on resource investment. This method provides a systematic way to assess alternative future perspectives and collect reliable data for scientific purposes based on the experts' views. Since its first appearance, the Delphi approach has undergone numerous revisions. It has been adapted not only to align with the nature and objectives of the research but also to meet specific goals, such as shortening the process and ensuring participant involvement throughout the rounds (Yusuwan et al., 2021). Despite some variations, the main characteristics of the Delphi method are consensual, including expert anonymity, controlled feedback, and repeated interactions. Typically, two to four rounds are required to reach a consensus (Avela, 2016; Chang et al., 2020; Demlehner et al., 2021).

Fig. 1 presents an overview of the Delphi method and research design adopted in this study. Specifically, a version of the Delphi method also known as the modified or hybrid Delphi method was adopted (Avela, 2016; Disconzi & Saurin, 2022; Landeta et al., 2011; Luoma et al., 2022). Unlike the traditional Delphi technique, the modified Delphi method does not rely on the expert panel to generate an initial response. Instead, the researcher first compiles responses from various sources, such as a comprehensive literature review, to develop a preliminary set of statements. This curated list is then provided to the expert panel at the start of the Delphi process (Avela, 2016). This approach reduces the cognitive load on experts during the initial phase while ensuring that the content reviewed is grounded in existing evidence and theory. While maintaining the flexibility of the traditional Delphi method by allowing experts to add, remove, or amend statements, the modified Delphi approach enhances the efficiency of the consensus-building process and ensures that the initial framework is comprehensive and research-based. Previous studies have used the Delphi method similarly. Nayak et al. (2021) designed a questionnaire to identify organizational factors influencing competitive advantage in health insurance firms, integrating them with structured interviews. Sillman et al. (2023) identified transaction factors in the Finnish energy systems through a workshop instead of asking open-ended questions to panelists, while the researchers in the work by Berbel-Vera et al. (2022) proposed their initial

conceptualization of statements related to key Chief Digital Office functions and then had them validated with support from literature and workshops. Luoma et al. (2022) proposed the first-round questionnaire based on a systematic review of the literature on the role of data in the circular economy, whereas Disconzi and Saurin (2022) started with a literature review of human factors to collect the principles of design for resilient performance. Similarly, the Delphi method has been used in further studies for the identification of human factors (Foster et al., 2020; Kelly et al., 2023). Nowadays, areas such as IT & cybersecurity increasingly require careful planning for a future that integrates research and organizations (Chowdhury et al., 2022).

In the following paragraphs, each stage of the research design is detailed.

Development of future projections

The conceptual background described in Section “Background” and the hypothetical statements for the First round questionnaire instrument were developed based on a systematic review of the literature on the role of humans in cybersecurity. This review was supplemented by recent research on human factors in cybersecurity and analyses of recent cyber incidents. The identified dimensions were integrated into the questionnaire items, which were formulated as statements for estimation tasks. A draft of the projections and questionnaire was then prepared. To ensure relevance, coverage, and a reasonable number of items, the wording was refined through an iterative process with the research group and pilot respondents during a pilot test (Rowe & Wright, 2001). The final questionnaire (Appendix A) for the First round of the Delphi process consisted of 19 statements, each offering the opportunity to recommend tools and best practices for future implementation, two open-ended questions, and a series of questions designed to profile the respondents.

Selection of panelists

The Delphi method facilitates meaningful assessments and predictions about potential future developments by experts (Tiberius et al., 2022). Therefore, selecting knowledgeable, experienced experts willing to participate throughout the study and able to articulate their views effectively is crucial (Disconzi & Saurin, 2022). Based on these premises, the experts were invited according to the following criteria:

- scholars specializing in cybersecurity, particularly those interested in human factors and vulnerabilities, who have published at least one article in peer-reviewed journals on these topics. Their expertise was verified using Scopus, a leading academic database with over 90 million records across 29,000 journals, sourced from more than 7000 publishers (RELX, 2023);
- practitioners working in areas such as risk management, IT systems, human resources, and business management, who have been involved in at least one cybersecurity-related project (e.g., cybersecurity training for employees). These individuals were identified using LinkedIn, a prominent professional networking platform (Iqbal & Ahmad, 2019). While years of cybersecurity experience were not a primary criterion, all experts were required to have at least three years of general experience, either in research or practice. This minimum experience requirement recognizes the evolving nature of the field and the value of recent entrants' perspectives. These experts were contacted via email.

Execution of Delphi study

All selected experts were invited to complete the First round of the questionnaire online. To clarify the study's objectives, all participants were provided with an introduction to the Delphi technique and the research objectives. The introduction can be found in Appendix A. Following the introduction, the experts rated all 19 statements

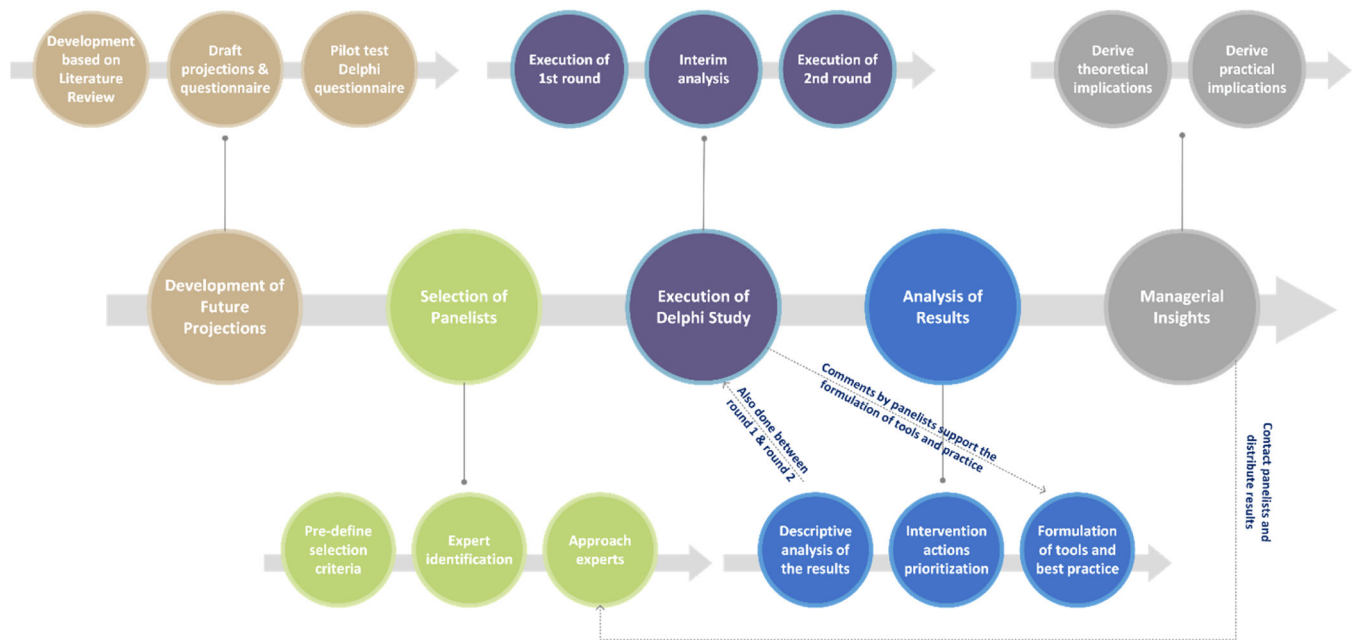


Fig. 1. Research Design adapted from Kluge et al. (2020), Luoma et al. (2022), Schmalz et al. (2021).

quantitatively based on the perceived importance of the interventions. In addition, for each statement and using an open-ended question, the participants were asked to indicate any personal experiences, tools, and best practices that can be used to implement each specific action. Finally, some open-ended questions allowed the participants to suggest additional actions that they felt had not been addressed by the 19 suggested statements.

An interim analysis followed the execution of the First round of the questionnaire, summarizing and aggregating the responses, for example, by identifying common new actions. The summarized responses were then reported back to the First round participants, along with an invitation to participate in the Second round of the questionnaire. This Second round included only the questions that had not reached consensus previously. For each of these questions, participants were provided with feedback on the group's mean responses, standard deviation, and median, as detailed in Appendix B. This feedback allowed participants to see how the overall group responses were distributed over each specific action, providing context for further evaluation. Participants also received a report containing both quantitative and qualitative results from the First round, including information on the statements that had reached a consensus. Studies have shown that informing participants about the aggregated opinions of others can improve the decision quality of the Delphi method (Berbel-Vera et al., 2022). They were then asked to score the importance of the actions using the same Likert scale.

Analysis of results

The analysis of the results began with a descriptive analysis of the responses collected, followed by an identification of those managerial actions that the experts had prioritized. As mentioned for quantitative analysis, the questions focused on the level of importance per action and the suggestions of best practices and tools. In line with previous studies (Berbel-Vera et al., 2022; Yusuwan et al., 2021), in each statement the respondents were asked to indicate the extent to which they felt investing resources was important for the future on a five-point Likert scale ranging from 1 (Not Important) to 5 (Very Important). The mean, together with standard deviation analysis, was used to determine a priority system for the intervention actions. The interquartile range was used as an indicator of consistency, with a threshold calculated based on

the number of levels of the Likert scale. To calculate the threshold, the approach proposed by Tiberius et al. (2022), which consists of multiplying the number of Likert scale levels by 0.25, was followed. Thus, for a 5-point Likert scale, 25 % of 5 is equal to 1.25. If the interquartile range exceeds this threshold, it indicates a lack of agreement on that item and, conversely, disagreement. The panel consensus was then assessed. The degree of consensus and degree of convergence were calculated through Eqs. (1) and (2), where Q1 and Q3 are the first quartiles and the third quartile coefficients, respectively.

$$\text{Degree of Consensus} = 1 - \frac{Q3 - Q1}{\text{medianvalue}} \quad (1)$$

$$\text{Degree of Convergence} = \frac{Q3 - Q1}{2} \quad (2)$$

To judge the agreement among the experts, a degree of consensus greater than 75 % and a degree of convergence lower than 50 % was considered (Berbel-Vera et al., 2022). Furthermore, a two-round process was defined to reach a consensus, in line with the suggestion by Mullen (2003) that no more than two rounds may be necessary when the sample is small. However, for further completeness, the content validity ratio (CVR) developed by Lawshe (1975) was calculated. The CVR is defined as the degree to which a sample of items taken together constitutes an adequate operational definition of a construct (Chang et al., 2020). The CVR was calculated according to Eq. (3), where N refers to the total number of experts and n_e refers to the number of experts who indicate that the item is essential (experts who selected "4 points" or "5 points").

$$\text{CVR} = \frac{n_e - (N/2)}{N/2} \quad (3)$$

A CVR value greater than zero indicates that more than 50 % of the panel members have agreed that an item is essential. However, according to Lawshe (1975), it is important to define a $\text{CVR}_{\text{critical}}$ to be used in the research. In this study, the number of experts was 29, which resulted in a $\text{CVR}_{\text{critical}}$ of 0.33.

Finally, the qualitative responses related to the formulation of tools and best practices shared by the experts were analyzed.

Managerial insights

In this last phase, the values for the managerial actions, as well as the new actions proposed by the experts, are discussed, and theoretical implications are derived. Moreover a cross-analysis of the tools and proposed best practices leads to the identification of practical implications to guide organizations in managing cybersecurity and to support them in their decision-making processes and in the future path of integrating people, processes, and technologies in cybersecurity.

Results

This section presents the results of the First and Second rounds of the Delphi study. Two rounds were considered sufficient to reach consensus, in line with previous studies involving small sample sizes as discussed in Section "Analysis of results". The presentation of results begins with an overview of the First Delphi round, outlining the composition of the expert panel and summarizing the initial findings. In this phase, consensus was achieved on 12 statements. Subsequently, the outcomes of the Second round are detailed, where consensus was reached on an additional five statements, while two statements remained without consensus. The final section (Section "Consensus on managerial actions") presents the experts' opinions on implementing the interventions, including the dissemination of tools and best practices for advancing cybersecurity management.

Descriptive statistics of participants

A total of 30 experts were invited to the initial round, with 29 submitting their responses. The Second round questionnaire was sent to these 29 respondents, and 26 participated in this subsequent phase of the Delphi process. Table 2 details the panelists' backgrounds as reported in the First round. The panel was composed of senior professors in the field of information security, researchers in the same field, experienced managers, and other personnel with industrial work experience covering organizational, IT, or risk management roles. The experts interviewed are part of international professional and academic networks operating across both the private and public sectors. While all the experts were based in Italy, the organizations involved in the study were also primarily Italian, but a few cases included Spanish, American, Swiss, and British companies. As for the other variables, there were 23 male and 6 female experts. The age range of the experts was evenly spread between 26 and 62 years. Nearly 70 % of the experts had been working for more than 10 years, with at least six years' experience in cybersecurity.

First-round results: key themes and initial consensus

Data analysis was conducted using values of the average, median, standard deviation, CVR, as well as the calculated change in these values between Round 1 and Round 2.

The First round was completed in 20 days (from December 11th to December 31st 2023). Consensus of agreement was reached on 12 statements (see Table 3). Specifically, 75 % of our experts agreed on 12 out of 19 statements. No consensus of disagreement was obtained. As noted earlier, comparisons between degrees of convergence, consensus, and critical CVR were made to assess the level of agreement. These analyses indicated that seven statements did not reach consensus, necessitating a second round. Furthermore, the experts reported that two statements overlapped. The expert panel suggested merging Statements 2 and 3 into one because they address both reducing cognitive fatigue and improving workload balance. They also suggested combining Statements 6 and 18 into one category because the latter is considered an instrument of the former. Finally, the experts proposed a new statement called "Responsible use of personal social network," scheduled for evaluation in the Second round.

Second round results: refinements and final consensus

The Second round was completed in 15 days, from February 12 to 26, 2024. Consensus was reached on five out of seven remaining statements (see Table 4). Therefore, overall, the study achieved consensus on 16 statements. Additionally, the experts agreed that the statement "Sharing success stories" was not essential. The action received a low score of importance and did not reach a consensus. As for "Dedicating staff to cybersecurity training," the experts did not reach a consensus, but their answers were sparse, reporting a greater interquartile range.

Finally, Table 5 displays the statements that have achieved consensus, listed in order of importance. For each action, the best practices and tools suggested by the experts in the open-ended responses that are useful for the dissemination of these interventions are shown in the right column.

Consensus on managerial actions

Encouraging personal responsibility

Encouraging personal responsibility is an important driver to improve cybersecurity by promoting a culture of vigilance together with proactive engagement in safeguarding it. Several practices and tools identified in the Delphi study can be leveraged to introduce these principles. A primary focus should be on implementing fear mitigation practices, which entails avoiding disciplinary methods following incidents that may breed resentment or foster disengagement. Instead, incentivizing incident reporting with rewards can encourage proactive engagement in sharing essential information. Practical training initiatives such as phishing simulations, and the introduction of gamified approaches, including competitions and gaming elements, are recommended. These methods inject dynamism and motivation into cybersecurity awareness efforts. Specifically, phishing attack simulations emerged as prominent strategies for enhancing preparedness and responsiveness without prior warning. Moreover, cybersecurity must not be viewed as a mere obligation but rather as a golden opportunity for personal and organizational growth, integrating mandatory training with spontaneous practice tests. A multifaceted approach encompassing education, simulation, gamification, and incentivization is recommended to encourage personal responsibility for cybersecurity.

Workload balance

Because the effectiveness of security practices depends on their integration with user workflows, several practices are suggested. One prominent approach involves aligning cybersecurity protocols with user convenience, exemplified by the adoption of biometric authentication as a user-friendly alternative to complex password requirements. Initiatives such as pre-alerting password change requests and the incorporation of physical device authentication help achieve a balance between security and usability. Additionally, centralizing strong authentication mechanisms and implementing Privileged Account Management simplifies security practices while ensuring robust protection of sensitive assets. Role-specific security standards, including differentiated approaches for top management and general staff, further contribute to workload balance by tailoring security measures to individual roles and responsibilities. Furthermore, the automation of vulnerability management processes and the implementation of specialized human resources reduce the burden on individual users while strengthening organizational defenses. Effective scheduling and workload distribution, facilitated by collaboration between IT departments and other managerial stakeholders, ensure that cybersecurity activities are integrated into existing workflows, as "effective planning reduces mental stress and heavy workloads (as a consequence of workload balancing) on one hand, and on the other, it tends to mitigate cyber risks (stemming from high mental stress situations)" (cybersecurity manager). In essence, the use of automation and a wise allocation of security measures emphasize the importance of harmonizing security measures with user workflows to achieve optimal cybersecurity outcomes.

Table 2
Panel demographics.

Characteristics	N = 29	
	n	%
Gender		
Female	6	21 %
Male	23	79 %
Age		
Under 30	6	21 %
30–39	9	31 %
40–49	5	17 %
50–59	7	24 %
Over 60	2	7 %
Work experience		
Less than 5 years	5	17 %
5–9 years	4	14 %
10–19 years	9	31 %
More than 20 years	11	38 %
Cybersecurity experience		
Less than 5 years	3	10 %
5–9 years	13	45 %
10–19 years	7	24 %
More than 20 years	6	21 %
Industry		
Academia	3	10 %
Banking, and Insurance	3	10 %
Chemistry & Pharmaceuticals	1	3 %
Consultancy	1	3 %
Oil & Gas	1	3 %
Transportation	3	10 %
Information Technology	9	31 %
Logistics	1	3 %
Media & Entertainment	1	3 %
Social Security	4	14 %
Public Administration & Defense	2	7 %
Area of Expertise^a		
Business Strategy	5	–
Information Technology	10	–
Operations Management	4	–
Cybersecurity	11	–
Risk management	5	–
Business size		
Micro (less than 10 employees)	3	10 %
Small (10 to 49 employees)	1	3 %
Medium (50 to 249 employees)	2	7 %
Large (at least 250 employees)	23	79 %
Job Title		
Chief Executive Officer	1	3 %
Chief Information Officer / Chief Technology Officer / Chief Information Security Officer	5	17 %
Cybersecurity / IT / Operations / Digital Strategy Manager	8	28 %
Cybersecurity / System / Risk Senior Consultant	3	10 %
Cybersecurity Junior Consultant / IT Junior Consultant	2	7 %

Table 2 (continued)

Characteristics	N = 29	
	n	%
Cybersecurity Engineer / Cyber Threat Analyst / Cybersecurity Penetration Tester	6	21 %
Cybersecurity Professor	1	3 %
Software and Systems Security / Visual Analytics for Cyber Security / Cybersecurity Researcher	3	10 %

^a A few experts expressed several areas of expertise.

Adopting models and standards

Cybersecurity models and standards represent desirable actions for effective cybersecurity management. These tools include community-developed websites such as OWASP and CWE for software development and vulnerability identification, respectively, and internationally recognized standards such as ISO 27001 for cybersecurity management systems. Additionally, the experts highlighted the role of AI technologies such as Darktrace in enhancing security. Moreover, frameworks such as COBIT were emphasized for their effectiveness in managing cybersecurity risks. Next-generation antivirus solutions, along with endpoint detection and response systems, were identified as essential for proactive threat detection and mitigation. Overall, the consensus among respondents emphasizes the importance of adhering to established standards, leveraging advanced technologies, and implementing robust management systems to bolster cybersecurity posture. However, as a cybersecurity researcher stated, *"I believe model and standards adoption is important, but only in cases where the right standard is applied to the right context."*

Awareness campaigns

Awareness campaigns represent another effective means to improve organizational cybersecurity. Owing to the ineffectiveness of universal approaches, the experts recommended tailoring awareness campaigns to specific target audiences. Moreover, the experts advocated for mandatory training with final tests to ensure comprehension, alongside interactive sessions such as tabletop exercises and simulations, which should leverage tools such as visors for enhanced engagement. Internal communications, including videos and group challenges, are recommended to reinforce cybersecurity messages. Additionally, specialized professional training is deemed essential to boost employee confidence and enthusiasm. Real-world anecdotes about phishing tools and procedures are recommended, with dedicated sessions led by experienced speakers to captivate the audience. Hence, the need for ongoing or permanent campaigns has been emphasized, and the experts agreed that the more these campaigns engage participants, the greater their impact.

Cybersecurity training

The experts provided valuable insights into effective tools and best practices for cybersecurity training, emphasizing the importance of authentic engagement and interaction as opposed to mere obligation. Interactive experiences such as escape rooms, simulations, phishing campaigns, and gaming activities were suggested as particularly effective methods for cybersecurity education. The participants noted that ongoing training efforts within organizations were producing substantial improvements in user attitude toward cybersecurity. They emphasized the need for training to be engaging, contextualized, and applicable outside the workplace. As a cyber threat analyst stated, *"the important thing is interactivity—something that truly engages personnel in a defense mindset and creates 'suspicion' in everyday activities that could conceal malicious actions."* Role-playing games have been suggested to educate employees on proper responses to cyberattacks, underscoring the interactive nature of effective training. Crisis management exercises, capture-the-flag competitions, and interactive simulations were recommended to enhance cybersecurity awareness and preparedness. Innovative approaches such as cartoons and interactive platforms were noted

Table 3

Round 1 results.

Round 1										
N.	Statement	Min	Max	Average	SD	Median	CVR	Degree of Convergence	Degree of Consensus	Consensus
A1	Encouraging personal responsibility	2	5	4,59	0,77,998	5	0,79,310,345	0,5	0,80	yes
A2	Reducing cognitive fatigue	2	5	3,66	0,85,673	3	−0,0,344,828	0,5	0,67	no
A3	Workload balance	1	5	3,69	1,22,776	4	0,31,034,483	1	0,50	no
A4	Adopting models and standards	3	5	4,28	0,79,716	4	0,5,862,069	0,5	0,75	yes
A5	Awareness campaigns	2	5	4,24	0,95,076	5	0,44,827,586	1	0,60	no
A6	Cybersecurity training	2	5	4,55	0,78,314	5	0,79,310,345	0,5	0,80	yes
A7	Dedicating staff to cybersecurity training	1	5	3,79	1,23,576	4	0,24,137,931	1	0,50	no
A8	Defining roles and responsibilities	1	5	4,21	0,90,156	4	0,72,413,793	0,5	0,75	yes
A9	Developing a cybersecurity-oriented culture	2	5	4,38	0,86,246	5	0,65,517,241	0,5	0,80	yes
A10	Encouraging feedback and peer learning	2	5	4,00	0,96,362	4	0,24,137,931	1	0,50	no
A11	Scheduling cybersecurity activities	2	5	3,76	0,98,761	4	0,17,241,379	1	0,50	no
A12	Sharing success stories	1	5	3,66	1,23,276	3	−0,0,344,828	1	0,33	no
A13	Simplifying Procedures	1	5	4,38	0,94,165	5	0,72,413,793	0,5	0,80	yes
A14	Team-level Cybersecurity Management	1	5	3,76	1,02,313	4	0,31,034,483	0,5	0,75	yes
A15	Adequacy of technical resources	3	5	4,48	0,78,471	5	0,65,517,241	0,5	0,80	yes
A16	Incident Reporting	3	5	4,59	0,68,229	5	0,79,310,345	0,5	0,80	yes
A17	Remote work cybersecurity	2	5	4,41	0,86,674	5	0,79,310,345	0,5	0,80	yes
A18	Simulation of cyber incidents	3	5	4,38	0,82,001	5	0,5,862,069	0,5	0,80	yes
A19	Understanding the limitations of cybersecurity devices	1	5	3,62	0,97,884	4	0,03,448,276	0,5	0,75	yes

Table 4

Round 2 results.

Round 2										
No.	Statement	Min	Max	Average	SD	Median	CVR	Degree of Convergence	Degree of Consensus	Consensus
A1	Encouraging personal responsibility	–	–	–	–	–	–	–	–	yes
A2	Workload balance	2	5	3,65	0,84,580	4	0,15,384,615	0,5	0,75	yes
A3	Adopting models and standards	–	–	–	–	–	–	–	–	yes
A4	Awareness campaigns	4	5	4,65	0,56,159	5	0,92,307,692	0,5	0,80	yes
A5	Cybersecurity training	–	–	–	–	–	–	–	–	yes
A6	Dedicating staff to cybersecurity training	2	5	3,92	0,89,098	4	0,46,153,846	0,75	0,63	no
A7	Defining roles and responsibilities	–	–	–	–	–	–	–	–	yes
A8	Developing a cybersecurity-oriented culture	–	–	–	–	–	–	–	–	yes
A9	Encouraging feedback and peer learning	3	5	4,04	0,72,004	4	0,53,846,154	0,375	0,81	yes
A10	Scheduling cybersecurity activities	3	5	4,30	0,53,349	4	0,92,307,692	0,5	0,75	yes
A11	Sharing success stories	2	5	3,31	0,97,033	3	0,07,692,308	0,5	0,67	no
A12	Simplifying Procedures	–	–	–	–	–	–	–	–	yes
A13	Team-level Cybersecurity Management	–	–	–	–	–	–	–	–	yes
A14	Adequacy of technical resources	–	–	–	–	–	–	–	–	yes
A15	Incident Reporting	–	–	–	–	–	–	–	–	yes
A16	Remote work cybersecurity	–	–	–	–	–	–	–	–	yes
A17	Understanding the limitations of cybersecurity devices	–	–	–	–	–	–	–	–	yes
A18	Responsible use of social network	2	5	4,30	0,91,903	4,5	0,69,230,770	0,5	0,78	yes

to improve training effectiveness, even though practical constraints such as budget and time must be considered. Participants agreed that these innovative approaches are more effective than traditional methods.

Additionally, the participants stressed the importance of frequent, in-person training sessions to ensure employee attention and information retention, cautioning against over-reliance on virtual tools such as VR, games, and chatbots. Red Teaming, penetration tests, tabletop exercises, and phishing simulations were highlighted as valuable contributions to cybersecurity training, emphasizing the importance of hands-on practice and real-world scenarios. Overall, the consensus among respondents underscores the need for dynamic, engaging, and interactive training methods to train employees about cybersecurity threats and best practices effectively.

Defining roles and responsibilities

According to the experts, defining roles and responsibilities is another important action to be taken to enhance cybersecurity within

organizations. The proposed practices encompass the application of the ISO 27,001 standard at an organizational level, ensuring a structured framework for delineating roles and responsibilities. Dedicated sessions aimed at explaining policies and clarifying defined roles were suggested to facilitate better understanding and adherence. These seminars are designed to establish a clear and shared operational model, fostering a culture of accountability and awareness across the organization. Additionally, periodic simulations of cybersecurity scenarios were recommended to assess individuals' adherence to the roles and responsibilities as outlined in security plans and policies. Importantly, the process of defining roles extends beyond the cybersecurity team to include members of other functions within the organization, emphasizing the importance of cross-functional collaboration in cybersecurity efforts. By presenting case studies of cyberattacks resulting from individual negligence and their repercussions, employees can gain awareness of the cascading effects of lapses in cybersecurity responsibilities. Overall, a standard reference system of roles and responsibilities, combined with

Table 5

Tools and best practices suggested by experts for each action.

No.	Statement	Average	Tools/Best Practice
A4	Awareness campaigns	4,65	Skill-wise awareness campaign; Mandatory awareness campaign; Tabletop; Simulation (e.g., Cyber drills); Virtual reality and Augmented Reality; CyberGuru courses; Active training
A1	Encouraging personal responsibility	4,59	Skill-wise awareness campaign; Short Security Pills; Simulations (e.g., Cyber Drills); Gaming; Competitions; Role-wise training
A15	Incident Reporting	4,59	Conditional reporting; CVE; Lesson Learned; Postmortem documents; Reports to corporate governance; Web portal for reporting potential incidents; Incident response plan; Preserving confidentiality; SOC reporting
A5	Cybersecurity training	4,55	Gaming (e.g., Escape Room, Role-playing Game); Simulation (e.g., Cyber ranges); Competition; Crisis management activities; Periodical training; Red Team–Blue Team activities / Hack-The-Box training; Role-playing game; Tabletop; Disaster & recovery demo; Endpoint Detection and Response
A14	Adequacy of technical resources	4,48	Privileged Account Management; AI Tools (e.g., CyberArk for user behavior analysis); Outsourcing SOC; Secure System Development Life Cycle Standard
A16	Remote work cybersecurity	4,41	System hardening (e.g., VPN, multifactorial identification, USB restrictions); Antivirus; Management of Virtual Desktop Infrastructure; Revising cybersecurity training content (e.g., including details on remote working activities); Alerts; Mandatory certifications
A8	Developing a cybersecurity-oriented culture	4,38	Newsletter; ISO27001; Sharing cyber incident stories; Endorsement by the top management
A12	Simplifying Procedures	4,38	Avoiding language gaps; Gaming; Use of images; Role-playing game; Audit
A3	Adopting models and standards	4,28	OWASP & CWE/SANS; ISO 27,001; ISA/IEC62443; AI Tools (e.g., AI Darktrace) Certification (e.g., FINCERT FIRST ISPE GAMP); COBIT; Next Generation Antivirus (NGAV)
A18	Responsible use of personal social network	4,26	Network Detection & Response (NDR)/Extended detection and response (XDR); Systems to protect the Cloud (e.g., Cloud Access Security Broker (CASB); Cloud Security Posture Management (CSPM)); Systems to prevent the dissemination of confidential information (DLP); Revising cybersecurity training content (e.g., including details on the use of social network); Revising policies and guidelines on the use of social network; Web filtering (ISO27001)
A7	Defining roles and responsibilities	4,21	ISO27001; Clear definition of roles and responsibilities through seminars
A9	Encouraging feedback and peer learning	4,04	Team discussions on cybersecurity best practices; One-to-one meetings; Feedback from cybersecurity team after evaluation

Table 5 (continued)

No.	Statement	Average	Tools/Best Practice
A10	Scheduling cybersecurity activities	3,76	test; Feedback on the actions not on the person/behavior; Sharing cyber incident stories
A13	Team-level Cybersecurity Management	3,76	Security by design; Scheduling a cybersecurity day; Penetration testing planning; Cybersecurity PMO; Risk management process; System hardening & patching; Including cybersecurity in the industrial strategic plan
A2	Workload balance	3,65	ISO 27,001; Key Risk Indicators (KRIs) / Cybersecurity Key Performance Indicators (KPIs) Biometric authentication; Privileged Account Management; Role-wise security standard; Differentiating Security Operations Center for top management; Simplifying guidelines and policies; H24 Outsourced SOC; Sharing cybersecurity activities scheduling
A17	Understanding the limitations of cybersecurity devices	3,62	Awareness campaign; Social engineering activities; Short Security Pills; Articles in the intranet; Security functional asset guide

ongoing seminars on its understanding and simulations of its implementation, are effective practices for defining roles and responsibilities in cybersecurity management.

Developing a cybersecurity-oriented culture

The experts agreed that developing a cybersecurity-oriented culture is essential for enhancing overall cybersecurity within organizations. Implementing an Information Security Management System (ISMS) based on the ISO 27,001 standard serves as a foundational step in fostering such a culture, as it provides a structured framework for cybersecurity practices and principles. Additionally, promoting transparency and clarity regarding cybersecurity matters and encouraging a shift towards sharing cyber incident stories with all personnel can significantly contribute to shaping a cybersecurity-focused culture. This entails periodic cyber risk assessments to assess organizational vulnerabilities as well as the endorsement of cybersecurity initiatives by top management through emails and newsletters, which would demonstrate leadership commitment to cybersecurity priorities. Moreover, targeted seminars and specialized professional training, facilitated by external cybersecurity experts, offer employees valuable opportunities to enhance their knowledge and skills, fostering a proactive and informed approach to cybersecurity. Engaging leadership, particularly at the board of directors level, in discussions on cybersecurity strategies and risk management further reinforces the organizational commitment to cybersecurity and cultivates a culture of accountability and vigilance. Through awareness campaigns, training, and ongoing communication efforts, organizations can instill a sense of responsibility for cybersecurity in employees and foster a culture where cybersecurity is integrated into every aspect of operations and decision-making processes.

Encouraging feedback and peer learning

Encouraging feedback and peer learning is recognized as a desirable action to enhance cybersecurity within organizations. The respondents suggest implementing evaluation tests with the opportunity for employees to provide suggestions on the improvement of cybersecurity practices. Additionally, facilitating team discussion on cybersecurity best practices allows for peer-to-peer knowledge sharing and learning from common security incidents. Sharing incident stories and providing personalized post-evaluation or post-incident feedback help employees

Table 6

Managerial actions transforming human factors from threat to opportunity.

Socio-technical perspectives	Managerial actions description	Human factors involved	Tools /Best practices
Individual	Encouraging personal responsibility This action addresses the tendency of individuals to feel insecure and avoid engaging in cybersecurity procedures. Individuals often rely on devices or people, mistakenly believing that these are the sole responsible for system security. Increasing awareness of individual responsibility in cybersecurity is critical to promoting a proactive approach to protecting corporate data and systems.	Complacency; Knowledge	Skill-wise awareness campaign; Short Security Pills; Simulations (e.g., Cyber Drills); Gaming; Competitions; Role-wise training
	Workload balance: The importance of workload management and effective scheduling of activities is emphasized to improve organizational cybersecurity. In situations of high mental stress or intense workload, employees are more likely to make mistakes due to distraction.	Distraction; Fatigue; Pressure; Resource; Stress	Biometric authentication; Privileged Account Management; Role-wise security standard; Differentiating Security Operations Center for top management; Simplifying guidelines and policies; H24 Outsourced SOC; Sharing cybersecurity activities scheduling
Organizational	Adopting models and standards: Identifying and sharing tools, such as recognized cybersecurity management frameworks and standards, which enable the organization to guide and manage its resources.	Resource	OWASP & CWE/SANS; ISO 27,001; ISA/IEC62443; AI Tools (e.g., AI Darktrace); Certification (e.g., FINCERT FIRST ISPE GAMP); COBIT; Next Generation Antivirus (NGAV)
	Awareness campaigns: Awareness campaigns contribute to effective cybersecurity by making people aware of the risks involved. In addition, these campaigns explain the rationale behind the policies, procedures, and practices in place. They may include informational materials, workshops, and specialized training.	Awareness; Norms	Skill-wise awareness campaign; Mandatory awareness campaign; Tabletop; Simulation (e.g., Cyber drills); Virtual reality and Augmented Reality; CyberGuru courses; Active training
	Cybersecurity training: Training increases knowledge for more effective cybersecurity. Employees, when trained, can be the main driver of more effective cybersecurity. Innovative approaches to training (e.g., VR, games, chatbots, simulation) were found to be slightly more effective in raising cybersecurity awareness.	Communication; Knowledge; Norms	Gaming (e.g., Escape Room, Role-playing Game); Simulation (e.g., Cyber ranges); Competition; Crisis management activities; Periodical training; Red Team–Blue Team activities / Hack-The-Box training; Role-playing game; Tabletop; Disaster & recovery demo; Endpoint Detection and Response
	Defining roles and responsibilities: Defining the roles and responsibilities of each employee, regardless of their areas of expertise, in cybersecurity plans and policies. This process includes assigning and explaining the required tasks, functions, and activities.	Communication	ISO27001; Clear definition of roles and responsibilities through seminars
	Developing a cybersecurity-oriented culture: Developing a cybersecurity-oriented organizational culture involves sharing strategic goals and communicating cybersecurity standards by linking them to corporate strategy.	Awareness; Communication; Knowledge; Teamwork	Newsletter; ISO27001; Sharing cyber incident stories; Endorsement by the top management
	Encouraging feedback and peer learning: In the context of cybersecurity, fostering a culture of feedback and peer learning is critical to creating a secure business environment. This exchange of mutual assessments can help to quickly address a cyber threat and establish a culture of security awareness among all employees.	Awareness; Communication; Knowledge; Teamwork	Team discussions on cybersecurity best practices; one to one meetings; Feedback from cybersecurity team after evaluation test; Feedback on the actions not on the person/ behavior; Sharing cyber incident stories
	Scheduling cybersecurity activities: Organizations that adopt multiple IT applications and devices do not often include specific cybersecurity training associated with them. Scheduling time for this activity will make the use of these devices more effective and secure.	Knowledge	Security by design; Scheduling a cybersecurity day; Penetration testing planning; Cybersecurity PMO; Risk management process; System hardening & patching; Including cybersecurity in the industrial strategic plan
	Simplifying Procedures: Security policies and procedures are often filled with technical language and information that can be difficult to understand. This complexity requires employees to invest time and effort into becoming familiar with these policies. Simplified communication of these procedures by the organization may reduce the burden on employees and improve the effectiveness of the policies themselves.	Pressure; Stress	Avoiding language gaps; Gaming; Use of images; Role-playing game; Audit
Technological	Team-level Cybersecurity Management: Aligning cybersecurity objectives at team level is crucial. A stronger team culture is suggested, where cybersecurity-related Key Performance Indicators (KPIs) are defined, incidents and difficulties communicated, and cybersecurity is integrated into daily team activities.	Assertiveness; Communication; Knowledge; Stress; Teamwork	ISO 27,001; Key Risk Indicators (KRIs) / Cybersecurity Key Performance Indicators (KPIs)
	Adequacy of technical resources: It is essential that the organization takes responsibility for ensuring that staff have access to all the information, financial and material resources needed to do their jobs. In the context of cybersecurity, this includes maintaining all systems to ensure effective defense against cyber-attacks. The availability of adequate technical resources and their proper	Resource	Privileged Account Management; AI Tools (e.g., CyberArk for user behavior analysis); Outsourcing SOC; Secure System Development Life Cycle Standard;

(continued on next page)

Table 6 (continued)

Socio-technical perspectives	Managerial actions description	Human factors involved	Tools /Best practices
	allocation and maintenance are critical to enabling individuals to maintain a sound cybersecurity posture. Incident Reporting: An organization's cybersecurity can be significantly improved by changing the perspective on incident reporting, viewing it as a virtuous act rather than a source of shame for causing the incident. Creating an environment where incident reporting is encouraged and treated confidentially can help identify and mitigate vulnerabilities, thereby protecting the organization from potentially greater harm. Remote work cybersecurity: The proliferation of remote working requires organizations to rethink their training programs. In particular, companies need to supplement cybersecurity training with procedures specific to remote work. Understanding the limitations of cybersecurity devices: A lack of understanding of cybersecurity devices leads individuals to overestimate the effectiveness of these devices in providing complete protection and to overlook the need for human oversight. Improving the understanding of such devices will contribute to more effective cybersecurity management and active oversight. Responsible use of personal social network: Several experts have proposed introducing new rules to address the cyber risks associated with social networks such as Facebook and LinkedIn. These risks arise from a lack of corporate guidelines, inappropriate behavior, and limited knowledge of social media, which can affect both individuals and companies. This scenario prompts reflection on a future where training, whether traditional or innovative, must address situations where attacks on the corporate network may originate from private social networks. It highlights the rules and behaviors for using social networks and sharing personal and corporate information.	Communication; Teamwork Distraction Distraction; Complacency; Knowledge Knowledge; Distraction; Awareness; Norms	Conditional reporting; CVE; Lesson Learned; Postmortem documents; Reports to corporate governance; Web portal for reporting potential incidents; Incident response plan; Preserving confidentiality; SOC reporting System hardening (e.g., VPN, multifactorial identification, USB restrictions); Antivirus; Management of Virtual Desktop Infrastructure; Revising cybersecurity training content (e.g., including details on remote working activities); Alerts; Mandatory certifications Awareness campaign; Social engineering activities; Short Security Pills; Articles in the intranet; Security functional asset guide Network Detection & Response (NDR)/Extended detection and response (XDR); Systems to protect the Cloud (e.g., Cloud Access Security Broker (CASB); Cloud Security Posture Management (CSPM)); Systems to prevent the dissemination of confidential information (DLP); Revising cybersecurity training content (e.g., including details on the use of social network); Revising policies and guidelines on the use of social network; Web filtering (ISO27001)

understand the impact of errors and learn from their mistakes, encouraging a culture of responsibility. Importantly, feedback should always be constructive and positive, focusing on actions and incidents rather than blaming individuals. The participants advised against penalizing employees for falling victim to cyberattacks, but recommend encouraging and rewarding the reporting of incidents, which promotes transparency and a proactive cybersecurity mindset across the organization. More specifically, negative feedback should be given constructively and individually, while positive feedback can be shared with the team (or, in special cases, with the organization). As a cybersecurity analyst and penetration tester stated, *“it is very important not to condemn the employee who unintentionally facilitated a breach or data leak (provided their innocence has been verified.....), but it is equally important to hold them accountable for the future by informing them of how they should have acted. In fact, the way feedback is given in such cases is a very delicate matter.”* Overall, practicing open communication, continuous learning, and supportive feedback mechanisms empowers employees to actively contribute to cybersecurity efforts.

Scheduling cybersecurity activities

The experts recognized the strategic importance of scheduling cybersecurity activities in the enhancement of cybersecurity within organizations. They advocated for the establishment of a comprehensive process of risk management that encompasses measures such as software design, implementation of security countermeasures, effectiveness monitoring, and vulnerability remediation. Furthermore, they emphasized the necessity of integrating cybersecurity activities into broader organizational strategies, elevating their significance to the level of strategic industrial planning. This entails incorporating cybersecurity education and implementing key frameworks, such as SecOps, for secure development practices. Establishing a Control Tower or Project

Management Office (PMO) dedicated to overseeing cybersecurity initiatives ensures centralized supervision and coordination. Penetration testing planning and dedicated calendar blocks for cybersecurity-focused events are also recommended strategies. While acknowledging the challenges posed by the scale of operations in larger organizations, the participants underscored the importance of both targeted education and the exploitation of technologies such as Artificial Intelligence (AI) in the optimization of resource allocation towards cybersecurity awareness and training efforts. Moreover, it is recognized that *“there is a need to include the security-by-design approach in all company processes”* (cybersecurity senior consultant and visual analytics for cyber security researcher). By embedding security-by-design principles and limiting employee exposure to unsafe actions, organizations can proactively mitigate risks and foster a culture of cybersecurity awareness and readiness across all levels, making security one of the main drivers in the formulation of a company’s architectural, infrastructural, and organizational policies.

Simplifying procedures

The experts emphasized the importance of simplifying procedures as a strategic action to enhance cybersecurity within organizations. Recognizing that technical jargon and complex language can pose challenges to non-technical personnel, participants advocated for the elimination of anglicisms and the use of clear, concise instructions in the local language, preferably with accompanying illustrative visuals. They stressed the need for specialized training to familiarize employees with the appropriate cybersecurity terminology, alongside dedicated sessions aimed at explaining procedures in an accessible manner. Furthermore, participants recommended incorporating role-playing exercises and simulations of real-life scenarios to provide practical experience in navigating cybersecurity processes. Regular audits and reviews of

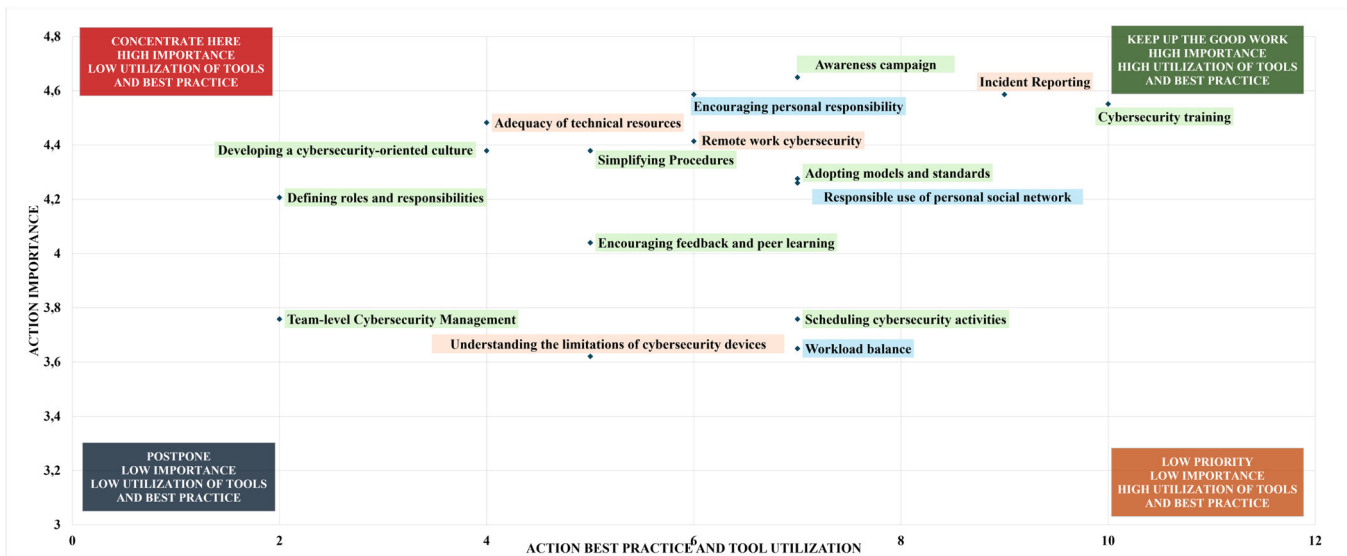


Fig. 2. Action importance–best practices and tools utilization graph.

security procedures are also recommended to identify areas for improvement and streamline governance models. While some caution against oversimplification, emphasizing the importance of precise communication, others underscore the need for user-friendly procedures tailored to the needs of diverse stakeholders. Ultimately, by simplifying procedures and fostering a culture of accessibility and clarity, organizations can empower employees to effectively adhere to cybersecurity protocols, thereby strengthening overall resilience against cyber threats.

Team-level cybersecurity management

Team-level cybersecurity management is considered a pivotal action for cybersecurity reinforcement. Central to this approach is the adoption and implementation of the ISO 27,001 standard, as it provides a structured framework for information security risks management. Participants advocated for the tailoring of Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) to assess the performance and effectiveness of cybersecurity functions at team level. Regular monitoring of these metrics enables teams to track their cybersecurity posture over time, identify areas for improvement, and respond promptly to cyber events. Moreover, the participants emphasized the necessity of ongoing engagement and training initiatives including workshops, seminars, and team-based exercises, to ensure that cybersecurity remains a continual focus for all team members. Dedicated cybersecurity teams or task forces are also recommended to provide specialized support and expertise and to foster a culture of collaboration and reliability. By establishing clear KPIs, implementing escalation procedures for incident response, and fostering a collaborative team environment, organizations can strengthen their cybersecurity resilience and mitigate risks effectively.

Adequacy of technical resources

The experts agreed that ensuring the adequacy of technical resources is a key action in the enhancement of cybersecurity. Central to this approach is the implementation of robust security management systems, such as the ISO 27,001 standard, which provides a structured framework for safeguarding information assets. The participants highlighted the importance of leveraging advanced technologies, including AI, to bolster security measures. AI-powered solutions offer the capability to analyze network behavior and detect anomalous activities, enabling timely alerts to security personnel for further investigation and response. Additionally, participants advocated for the establishment of dedicated roles, such as security architects, who should be responsible for the design and maintenance of security infrastructure in collaboration with external analysts from Security Operations Centers (SOC) and Computer

Emergency Response Teams (CERT). Meanwhile, the adoption of Secure System Development Life Cycle (SSDLC) principles ensures that security considerations are integrated into all stages of technology deployment and development processes. Technical resources such as AI, antivirus software, and other tools are essential because, without these, personnel would struggle to manage cybersecurity effectively. Merely relying on individual abilities does not suffice: employees also need adequate technical resources and proper training on how to use them.

Incident reporting

The experts underscored the pivotal role of incident reporting in fortifying cybersecurity. They advocated for a multifaceted approach to incident reporting, emphasizing the importance of timely communication and structured documentation throughout the process. A key aspect is the conditionality of incident reporting based on the severity of vulnerabilities or the actual impact of the attack on the system. This nuanced approach ensures that resources are allocated appropriately and critical security threats are addressed effectively. Furthermore, the incorporation of post-incident analysis, such as post-mortem and lessons-learned documents, facilitates continuous improvement and knowledge sharing within the organization. The participants also stressed the importance of confidentiality in incident reporting, ensuring that employees feel empowered to report incidents without fear of repercussions. This entails implementing secure reporting channels and limiting access to sensitive information to authorized personnel only. Additionally, the integration of incident reporting mechanisms with Security Operations Centers (SOC) and Computer Emergency Response Teams (CERT) streamlines response efforts and facilitates collaboration among relevant stakeholders. Regular reporting of incidents, coupled with periodic reviews and revision of Key Performance Indicators (KPIs), enables organizations to monitor their cybersecurity posture effectively and refine incident response strategies over time. Ultimately, incident reporting serves as a cornerstone in fostering a proactive cybersecurity culture, promoting transparency, accountability, and collective resilience against evolving cyber threats.

Remote work cybersecurity

According to our experts, addressing remote work cybersecurity is an action to be undertaken to support the overall cybersecurity posture. The unanticipated widespread adoption of remote work due to the COVID-19 pandemic compelled millions of employees to operate in environments and with tools that might not have always met optimal security standards. While organizations invest in technologies and

Table 7
Tools and best practices impact on actions (excerpt).

Tool or Best Practice proposed by the experts	Awareness campaigns	Encouraging personal responsibility	Incident Reporting	Cybersecurity training	Adequacy of technical resources	Remote work cybersecurity	Developing a cybersecurity-oriented culture	Simplifying Procedures	Adopting models and standards	Responsible use of personal social network	Defining roles and responsibilities	Encouraging feedback and peer learning	Scheduling cybersecurity activities	Team-level Cybersecurity Management	Workload balance	Understanding the limitations of cybersecurity devices	
ISO2700X							X		X	X	X			X			5
Role-wise awareness campaign	X	X														X	3
Simulation (e.g., Cyber Drills / Cyber Ranges)	X	X		X													3
Gaming (e.g., Escape Room, Role-playing Game)		X		X				X									3
Role-wise training		X		X				X									3
Mandatory awareness campaign	X															X	2
Tabletop / Crisis Management Activities	X			X													2
Short Security Pills		X														X	2
Competitions		X		X													2
Threat Detection and Response Solutions (e.g., Endpoint Detection and Response (EDR); Network Detection & Response (NDR); Extended detection and response (XDR))				X						X							2
AI Tools (e.g., CyberArk for user behavior analysis; Darktrace AI to uncover threats)					X				X								2
Outsourcing h24 SOC					X										X		2
Privileged Account Management					X										X		2
System hardening & patching (e.g., VPN, multifactorial identification, USB restrictions)						X							X				2
Antivirus (e.g., Next Generation Antivirus NGV)						X			X								2
Revising cybersecurity training content (e.g., include details on remote working activities; use of social network)						X				X							2
Mandatory external certifications						X						X					2
Newsletter / Articles in the Intranet							X									X	2
Sharing cyber incident stories							X					X					2
Risk management process / Key Risk Indicators (KRIs) / Cybersecurity Key Performance Indicators (KPIs)													X	X			2

processes to safeguard their information assets, individuals can apply these measures effectively, which will ultimately make a difference. Key solutions and best practices identified by the participants include implementing stringent system hardening measures, such as VPN with multifactor authentication and USB restrictions, to secure remote connections. Moreover, centralized management of Virtual Desktop Infrastructure (VDI) and enhanced monitoring by Security Operations Centers (SOC) using technologies such as Machine Learning to detect anomalous user behavior contribute to a more secure remote work environment. Mandatory training on cyber vulnerabilities related to remote working along with the requirement for remote access certification highlights the high level of attention organizations dedicate to remote work security. The implementation of Multi-Factor Authentication (MFA) and the utilization of technologies such as Endpoint Detection and Response (EDR), web filtering, and email security further fortify remote work environments. The emphasis on sharing best practices and providing straightforward instructions to users, coupled with the deployment of appropriate remote work technologies, forms a holistic approach to enhancing remote work cybersecurity. By integrating these strategies, organizations can mitigate risks and ensure the security and productivity of remote work arrangements.

Understanding the limitations of cybersecurity devices

The experts recognized that understanding the limitations of cybersecurity devices is crucial in the enhancement of overall cybersecurity. The widespread adoption of remote work has highlighted the necessity for organizations to deploy robust security measures tailored to the unique challenges of remote environments. While organizations invest in technologies and processes to protect their information assets, stakeholders must comprehend the inherent limitations of these cybersecurity devices. This understanding enables organizations to effectively evaluate the efficacy of existing security measures and identify areas for improvement. Key solutions and best practices identified by the participants include implementing stringent system hardening measures, such as VPN with multifactor authentication and USB restrictions, to secure remote connections. By acknowledging and addressing the limitations of cybersecurity devices, organizations can develop more resilient cybersecurity strategies and prevent employees from over-trusting these devices.

Responsible use of personal social networks

The theme of social networks and cybersecurity is becoming increasingly relevant due to the widespread use of platforms and the growing user base, who begin at a younger age. It is therefore important to incorporate security topics into training and prevention programs to address potential cyberattacks. Implementing rules and templates for whatever can be shared on social networks is crucial. Sensitization (and awareness) campaigns with realistic practical examples are essential to truly convey the devastating impact of cyberattacks. There is often a lack of awareness of the implications of sharing personal information on social networks, especially concerning the security of the organization one works for. Attention should also be given to regulatory aspects, particularly regarding the use of social media in the workplace. Although this may be more relevant for companies with mobile devices operating on corporate VPNs, it is still important to consider the consequences for all companies. Social networks serve as abundant sources of information for conducting attacks such as business email compromise (BEC). Thus, web filtering systems are essential, as evidenced by their inclusion in the 2022 version of ISO27001. As reported by a Chief Information Security Officer, *“One of the attacks observed in the past originated directly from LinkedIn, through a fabricated job position and the exchange of a Word document containing an infostealer. However, our XDR solution successfully prevented the execution of the malware, enabling us to reconstruct all events of the attack. Social networks are integral parts of our lives and pose an increasing cyber risk, amplified by the introduction of AI. Corporate training should encompass the risks and behaviors to adopt on*

these platforms. Several colleagues have highlighted how this training has significantly benefited their personal sphere as well.”

Discussion

At the end of the Delphi study, the experts reached a consensus on 16 critical managerial actions to be taken to enhance the role of humans in cybersecurity management. This confirms a significant paradigm shift over recent years (Edeh, 2023; Pawlicka et al., 2022; Rahman et al., 2021). The research presents several insights, which can be categorized into theoretical and practical contributions.

Theoretical contributions

The managerial actions that emerged from the study, qualitatively described in Section "Consensus on managerial actions", contribute to the ongoing debate regarding the role of people in cybersecurity—whether as a source of threat or as solutions to cybersecurity vulnerabilities (Desolda et al., 2021b; Zimmermann & Renaud, 2019). Specifically, the actions aim to enhance cybersecurity by using human factors potential, which addresses the research objective.

Viewed through the lens of socio-technical systems theory (Malatji et al., 2019; Patriarca et al., 2021), and in line with Pollini et al. (2022), the proposed actions are categorized into three perspectives: individual, organizational, and technological.

Therefore, the managerial actions identified contribute to both behavioral security theory and human-computer interaction theory, offering a socio-technical perspective on the actions needed to leverage human factors in improving cybersecurity.

Table 6 outlines the above-mentioned perspectives, the suggested actions, the human factors involved, and the tools and best practices that can facilitate the implementation of the actions.

Practical contributions

The experts offered several takeaways for organizations dealing with emerging cybersecurity issues and agree that practitioners and scholars should view humans as integral solutions to cybersecurity challenges rather than vulnerabilities (Zimmermann & Renaud, 2019). In addition, the experts established a prioritization hierarchy for resource allocation to these interventions, acknowledging the financial and temporal constraints organizations face when implementing effective cybersecurity strategies (Annarelli et al., 2021; Chidukwani et al., 2022). By answering open-ended questions, the participants shared their insights and experiences, highlighting tools and best practices that can help organizations overcome future cybersecurity challenges.

Fig. 2 categorizes these intervention actions based on the urgency of investment (y-axis) and the availability of supporting tools or best practices (x-axis). The y-axis, labeled “Action Importance,” represents the experts’ ratings of each intervention action on a scale of 1 to 5, indicating how critical they consider it to prioritize or invest in the corresponding business objectives. The x-axis, labeled “Action Best Practice and Tool Utilization,” indicates the number of tools and best practices recommended by the experts for each action. A higher value on this axis suggests that these actions are already being extensively addressed and implemented by practitioners through the use of specific tools and best practices. The diagram displays four separate quadrants. The first quadrant, “Concentrate here,” highlights the need for urgent attention to high-priority actions with limited support, such as fostering a cybersecurity-inclusive organizational culture and clarifying cybersecurity roles and responsibilities. These actions have limited tools or best practices available, which makes them a critical focus for the cybersecurity community. The second quadrant, “Keep up the good work,” emphasizes sustaining momentum on actions already supported by effective tools, such as ongoing cybersecurity training and incident reporting mechanisms. Effective tools identified for cybersecurity

training include simulation exercises, gaming, role-specific training, tabletop exercises, and competitions (Fig. 2). For incident reporting, the experts suggested tools include lessons learned documents, incident response plans, web portals, post-mortem analysis, and SOC (Security Operations Center) reporting (Appendix C). The framework also identifies lower-priority areas, labeled “Postpone” and “Low Priority,” which may require future investment. These actions encompass team-level cybersecurity management, fostering feedback and peer learning and maintaining workload balance. They are especially crucial for SMEs, where priorities must be carefully managed (Armenia et al., 2021). The framework serves as a strategic guide for both established entities looking to improve their cybersecurity investments and nascent firms navigating initial resource allocation.

A subsequent visualization, Table 7 (Table 7 is an extraction of the full table (Table C.1) that can be found in Appendix C) details the 44 tools and 26 best practices identified by the experts, highlighting a balanced approach that goes beyond technical solutions to include mindsets and procedural shifts (Blair et al., 2019; Jeong et al., 2019). Notable examples include the ISO27000 series and innovative engagement methods such as role-wise and skill-specific gamification and simulations, which are effective in fostering a cybersecurity culture. Furthermore, effective knowledge transfer is achieved through role-specific and skill-specific campaigns and training. When addressing complex topics like this, it is essential to engage individuals by tailoring the proposal to their skills (Dincelli & Chengalur-Smith, 2020; Erdogan et al., 2021). Continuous learning is necessary due to the constant emergence of news on cybersecurity, new threats, and attack techniques (Annarelli et al., 2020; Prümmer et al., 2024). Short security training sessions, small-scale training, or periodic communications (e.g., short security pills) are recommended. Moreover, the findings suggest a holistic approach to cybersecurity, advocating for the integration of technology-driven solutions such as AI for behavior analysis and attack detection within a broader framework that prioritizes human-centric strategies and continuous skill development. A comprehensive table of tools and practices (Table C.1) illustrates potential synergies across multiple intervention actions, offering a roadmap for targeted and efficient future investments in cybersecurity.

A practice that emerged from the study is the use of simulation and gamification to drive engagement and facilitate learning. This observation, corroborated by the experts, aligns seamlessly with existing literature. Engagement stands out as a strength of the game and simulation-based training programs, albeit requiring regular updates to address new threats and vulnerabilities, and often targeting specific user groups and roles (Jayakrishnan et al., 2022; Jin et al., 2018; Nagarajan et al., 2012; Sheng et al., 2007; Tonkin et al., 2023). While not groundbreaking, this insight underscores the relevance and contemporary perspective of our experts, demonstrating alignment with current best practices. An innovative practice identified involves the optimal way to provide feedback on cybersecurity, encouraging incident reporting and knowledge sharing. By enabling individuals to report incidents privately, receive feedback individually, and communicate anonymously within the company, it is possible to reduce the stigma associated with being a cybersecurity incident victim. Furthermore, it is possible to incentivize the sharing of positive experiences (e.g., an avoided attack) by collectively giving positive feedback and prizes. These mechanisms induce organization members to collaborate in reporting positive and negative experiences. By means of intra- and inter-company networks, the experiences can be used internally and externally to prevent adverse events and behaviors. Another key insight pertains to the necessity of targeting cybersecurity resources and processes according to specific roles to ensure effectiveness. Simplified language for non-experts, role-specific training, and access to targeted information and technologies can streamline cognitive information processing and mitigate risky behaviors, effectively distributing responsibility. By implementing these strategies, organizations can empower employees to play an active role in cybersecurity and

transform threats into opportunities.

Conclusions and future steps

This research marks a significant advance in understanding the critical role of humans in enhancing cybersecurity management within organizations. The Delphi method facilitated expert consensus on 16 key intervention actions that represent a paradigm shift in the cybersecurity domain. This shift recognizes humans as essential components of cybersecurity solutions, rather than merely as sources of vulnerabilities. The findings underscore the need for a comprehensive, human-centered approach that integrates technological tools with strategic human interventions to foster a robust cybersecurity culture. The analysis presents a prioritized roadmap for organizations to effectively implement human-focused interventions and defend their information systems. It highlights the importance of continuous learning, the development of a cybersecurity-inclusive organizational culture, and the clarification of roles and responsibilities within the cybersecurity framework (Tejay & Mohammed, 2023).

Despite its contributions, this study has certain limitations and offers directions for future research. Increasing the sample size of experts involved in the Delphi study could enhance the robustness of the findings. Moreover, practical assessments are essential to guide companies in implementing the identified intervention strategies effectively. Future research should also focus on developing conceptual frameworks or models that organizations can use to integrate human factors into their cybersecurity strategies efficiently.

Acquiring quantitative data on the effectiveness and adoption of proposed tools will be crucial in validating their impact on cybersecurity postures. Additionally, addressing privacy concerns within these frameworks could ensure that the strategies are adaptable across different regulatory environments, further protecting organizations against cyber threats. Finally, exploring less developed intervention actions, where current tools and practices fall short, could lead to innovative solutions that strengthen cybersecurity resilience.

Disclosure of interests

The authors declare that they have no conflict of interests to declare.

Funding

This work was supported by projects: SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union - NextGenerationEU.

CRedit authorship contribution statement

Silvia Colabianchi: Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Software, Project administration, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Francesco Costantino:** Writing – review & editing, Writing – original draft, Validation, Supervision, Resources. **Fabio Nonino:** Writing – review & editing, Writing – original draft, Validation, Supervision, Resources. **Giulia Palombi:** Writing – review & editing, Writing – original draft, Validation, Supervision, Project administration, Methodology, Investigation, Formal analysis, Data curation, Conceptualization.

Acknowledgments

The authors thank the master thesis students involved in the study. Specifically, the authors thank Luigi Andrea Verardi for his contribution to the literature background and Kerolus Kaldas for structuring the Delphi study and analysis.

Appendix A

Delphi Questionnaire – Round 1

Cybersecurity: the key role of humans and possible intervention actions

Introduction

Cybersecurity has become an increasingly important issue for public and private organizations and institutions. In the fight against cyber threats, there is often a tendency to focus on technical factors while neglecting the key role that people play in cybersecurity.

We therefore asked ourselves:

- How can people be a solution to (rather than a problem for) cybersecurity?
- Is it possible to adopt good management practices, as well as preventive, reactive, and corrective measures that integrate people with technologies and processes?

Traditionally, human factors such as communication, stress, fatigue, and awareness are considered the weakest link in cybersecurity. However, recent studies show that incorporating human factors into cybersecurity is a key step in the development of a holistic approach to the subject. This study, using the Delphi methodology, aims to gather expert opinions and experiences on the importance and implementation of some intervention actions identified in the literature to rethink the human role in cybersecurity.

The results of the study, by integrating theoretical findings from the scientific literature and the opinions of experts in the field, will provide a basis for the development of targeted security strategies, effective training programs, and corporate policies aimed at reducing vulnerabilities and improving the human role in cybersecurity management.

Once the study is complete, the results will be shared with the participants.

Part 1. Respondent profile

The purpose of this section is to gather information about the professionals who will participate in the survey.

1. Age __
2. Gender:
 - M
 - F
 - Other
3. Do you have a bachelor's degree? Yes No
4. If yes, which one? __
5. What postgraduate degrees have you obtained?
 - Ph.D.
 - MBA or Executive MBA
 - Other
 - No postgraduate degree
6. How many years have you worked?
7. How many years have you worked on cybersecurity issues?
8. Current position (job title) __
9. Is there more than one person on your team? If so, how many? __
10. Are you the team coordinator? Yes No
11. Size of organization:
 - Micro (less than 10 employees)
 - Small (10 to 49 employees)
 - Medium (50 to 249 employees)
 - Large (250 or more employees)
12. Field of expertise:
 - IT
 - Risk management
 - Human Resources
 - Business Management
 - Other: _____
13. Current employment sector (industry):
 - Information Technology and Telecommunications
 - Logistics
 - Electronics
 - Mechanical and engineering
 - Academia
 - Public Administration & Defense
 - Communication
 - Commerce
 - Administration
 - Agribusiness
 - Banking & Insurance

- Chemistry & Pharmaceuticals
- Personal services
- Textile, Leather & Fashion
- Others: _____

Part 2. Importance of intervention actions

Below are 19 intervention actions identified in the literature for leveraging human potential for organizational cybersecurity.

Looking ahead, please carefully assess each of these intervention actions on a scale of 1 to 5, indicating how important/prioritized **you believe it should be to invest and/or focus on the business objectives associated with each action.**

This assessment will result in a targeted cybersecurity strategy tailored to your organization's specific needs. Given the current business scenario, with often limited resources, it is not always possible to act on every action, but it is necessary to make judicious choices based on their importance and the resources available.

For each intervention action, it is therefore necessary to

A. Rate its importance from 1 to 5 *.

B. Provide any tools and best practices that can be useful to implement it in the future.

At the end of the questionnaire, participants will also have the opportunity to suggest additional intervention actions.

**1 means "not important" and 5 means "very important."*

1.A. Encouraging personal responsibility

This intervention action addresses the tendency of individuals to feel insecure and avoid engaging in cybersecurity procedures. Individuals often rely on devices or people, mistakenly believing that these are the sole responsible for system security. Increasing awareness of individual responsibility in cybersecurity is critical to promoting a proactive approach to protecting corporate data and systems.

How important/prioritized do you think it should be to invest in or focus on this action in the future?

- 1 (not important)
- 2 (slightly important)
- 3 (moderately important)
- 4 (important)
- 5 (very important)

1.B. Please indicate any tools and best practices that have already been implemented in your organization, or that you would like to propose for the future, that could be useful to encourage personal responsibility.

2.A. Reducing cognitive fatigue.

Cognitive fatigue represents the maximum number of cognitive resources an individual can devote to security issues. Multiple policies and procedures can cause fatigue in employees who may feel stressed and exhausted due to excessive pressure and oversight in the workplace. Cognitive fatigue and associated cyber risks can be mitigated by properly balancing the number of norms when they are brought to the attention of employees (e. g., password changes).

How important/prioritized do you think it is to invest in or focus on this action in the future?

- 1 (not important)
- 2 (slightly important)
- 3 (moderately important)
- 4 (important)
- 5 (very important)

2.B. Please indicate any tools and best practices that have already been implemented in your organization, or that you would like to propose for the future, that could be useful to reduce cognitive fatigue.

3.A. Workload balance

The importance of workload management and effective scheduling of activities is emphasized to improve organizational cybersecurity. In situations of high mental stress or intense workload, employees are more likely to make mistakes due to distraction. Therefore, it is essential to balance workloads and plan activities wisely to ensure a more secure organizational environment.

How important/prioritized do you think it should be to invest in or focus on this action in the future?

- 1 (not important)
- 2 (slightly important)
- 3 (moderately important)
- 4 (important)
- 5 (very important)

3.B. Please indicate any tools and best practices that have already been implemented in your organization, or that you would like to propose for the future, that could be useful for workload balancing.

4.A. Adopting models and standards

Identifying and sharing tools, such as recognized cybersecurity management frameworks and standards, which enable the organization to guide and manage its resources.

How important/prioritized do you think it should be to invest in or focus on this action in the future?

- 1 (not important)
- 2 (slightly important)
- 3 (moderately important)
- 4 (important)
- 5 (very important)

4.B. Please indicate any tools and best practices that have already been implemented in your organization, or that you would like to propose for the future, that could be useful for the adoption of models and standards.

5.A. Awareness campaigns

Awareness campaigns contribute to effective cybersecurity by making people aware of the risks involved. In addition, these campaigns explain the rationale behind the policies, procedures, and practices in place. They may include informational materials, workshops, and specialized training.

How important/prioritized do you think it should be to invest in or focus on this action in the future?

- 1 (not important)
- 2 (slightly important)
- 3 (moderately important)
- 4 (important)
- 5 (very important)

5.B. Please indicate any tools and best practices that have already been implemented in your organization, or that you would like to propose for the future, that could be useful for advocacy/awareness campaigns.

6.A. Cybersecurity Training

Training increases knowledge for more effective cybersecurity. Employees, when trained, can be the main driver of more effective cybersecurity. Innovative approaches to training (e.g., VR, games, chatbots) were found to be slightly more effective in raising cybersecurity awareness.

How important/prioritized do you think it should be to invest in or focus on this action in the future?

- 1 (not important)
- 2 (slightly important)
- 3 (moderately important)
- 4 (important)
- 5 (very important)

6.B. Please indicate any tools and best practices that have already been implemented in your organization, or that you would like to propose for the future, that could be useful for cybersecurity training.

7.A. Dedicating staff to cybersecurity training.

Most organizations suffer from a lack of staff dedicated to cybersecurity awareness programs. Resources responsible for awareness programs are often involved in other activities and areas, which limits their ability to fully commit to employee training.

How important/prioritized do you think it should be to invest in or focus on this action in the future?

- 1 (not important)
- 2 (slightly important)
- 3 (moderately important)
- 4 (important)
- 5 (very important)

7.B. Please indicate any tools and best practices that have already been implemented in your organization, or that you would like to propose for the future, that could be useful to dedicate staff to cybersecurity training.

8.A. Defining roles and responsibilities.

Defining the roles and responsibilities of each employee, regardless of their areas of expertise, in cybersecurity plans and policies. This process includes assigning and explaining the required tasks, functions, and activities.

How important/prioritized do you think it should be to invest in or focus on this action in the future?

- 1 (not important)
- 2 (slightly important)
- 3 (moderately important)
- 4 (important)
- 5 (very important)

8.B. Please indicate any tools and best practices that have already been implemented in your organization, or that you would like to propose for the future, that could be useful to define roles and responsibilities.

9.A. Developing a cybersecurity-oriented culture.

Developing a cybersecurity-oriented organizational culture involves sharing strategic goals and communicating cybersecurity standards by linking them to corporate strategy.

How important/prioritized do you think it should be to invest in or focus on this action in the future?

- 1 (not important)
- 2 (slightly important)
- 3 (moderately important)
- 4 (important)
- 5 (very important)

9.B. Please indicate any tools and best practices that have already been implemented in your organization, or that you would like to propose for the future, that could be useful to develop a cybersecurity-oriented organizational culture.

10.A. Encouraging feedback and peer learning.

In the context of cybersecurity, fostering a culture of feedback and peer learning is critical to creating a secure business environment. This exchange of mutual assessments can help to quickly address a cyber threat and establish a culture of security awareness among all employees.

How important/prioritized do you think it should be to invest in or focus on this action in the future?

- 1 (not important)
- 2 (slightly important)
- 3 (moderately important)
- 4 (important)
- 5 (very important)

10.B. Please indicate any tools and best practices that have already been implemented in your organization, or that you would like to propose for the future, that could be useful to promote feedback and peer learning.

11.A. Scheduling cybersecurity activities.

Organizations that adopt multiple IT applications and devices do not often include specific cybersecurity training associated with them. Scheduling time for this activity will make the use of these devices more effective and secure.

How important/prioritized do you think it should be to invest in or focus on this action in the future?

- 1 (not important)
- 2 (slightly important)
- 3 (moderately important)
- 4 (important)
- 5 (very important)

11.B Please indicate any tools and best practices that have already been implemented in your organization, or that you would like to propose for the future, that could be useful for scheduling cybersecurity activities.

12.A. Sharing success stories.

The term "success stories" identifies those events where cybersecurity information sharing has made a significant difference. These include situations where participants prevented harm by sharing incident reports and information on previous attacks. Promoting and communicating such positive examples means recognizing those employees who identify potential attacks and/or report them to colleagues.

How important/prioritized do you think it should be to invest in or focus on this action in the future?

- 1 (not important)
- 2 (slightly important)
- 3 (moderately important)
- 4 (important)
- 5 (very important)

12.B. Please indicate any tools and best practices that have already been implemented in your organization, or that you would like to propose for the future, that could be useful to share success stories.

13.A. Simplifying Procedures

Security policies and procedures are often filled with technical language and information that can be difficult to understand. This complexity requires employees to invest time and effort into becoming familiar with these policies. Simplified communication of these procedures by the organization may reduce the burden on employees and improve the effectiveness of the policies themselves.

How important/prioritized do you think it should be to invest in or focus on this action in the future?

- 1 (not important)
- 2 (slightly important)
- 3 (moderately important)
- 4 (important)
- 5 (very important)

13.B. Please indicate any tools and best practices that have already been implemented in your organization, or that you would like to propose for the future, that could be useful to simplify procedures.

14.A. Team-level Cybersecurity Management

Aligning cybersecurity objectives at team level is crucial. A stronger team culture is suggested, where cybersecurity-related Key Performance Indicators (KPIs) are defined, incidents and difficulties communicated, and cybersecurity is integrated into daily team activities.

How important/prioritized do you think it should be to invest in or focus on this action in the future?

- 1 (not important)
- 2 (slightly important)
- 3 (moderately important)
- 4 (important)
- 5 (very important)

14.B. Please indicate any tools and best practices that have already been implemented in your organization, or that you would like to propose for the future, that could be useful for cybersecurity management at team level.

15.A. Adequacy of technical resources

It is essential that the organization takes responsibility for ensuring that staff have access to all the information, financial and material resources needed to do their jobs. In the context of cybersecurity, this includes maintaining all systems to ensure effective defense against cyber-attacks. The availability of adequate technical resources and their proper allocation and maintenance are critical to enabling individuals to maintain a sound cybersecurity posture.

How important/prioritized do you think it should be to invest in or focus on this action in the future?

- 1 (not important)
- 2 (slightly important)
- 3 (moderately important)
- 4 (important)
- 5 (very important)

15.B. Please indicate any tools and best practices that have already been implemented in your organization, or that you would like to propose for the future, that could be useful to ensure the adequacy of technical resources.

16.A. Incident Reporting

An organization's cybersecurity can be significantly improved by changing the perspective on incident reporting, viewing it as a virtuous act rather than a source of shame for causing the incident. Creating an environment where incident reporting is encouraged and treated confidentially can help identify and mitigate vulnerabilities, thereby protecting the organization from potentially greater harm.

How important/prioritized do you think it should be to invest in or focus on this action in the future?

- 1 (not important)
- 2 (slightly important)
- 3 (moderately important)
- 4 (important)
- 5 (very important)

16.B. Please indicate any tools and best practices that have already been implemented in your organization, or that you would like to propose for the future, that could be useful to promote incident reporting.

17.A. Remote Work Cybersecurity

The proliferation of remote working requires organizations to rethink their training programs. In particular, companies need to supplement cybersecurity training with procedures specific to remote work.

How important/prioritized do you think it should be to invest in or focus on this action in the future?

- 1 (not important)
- 2 (slightly important)
- 3 (moderately important)
- 4 (important)
- 5 (very important)

17.B. Please indicate any tools and best practices that have already been implemented in your organization, or that you would like to propose for the future, that could be useful for managing cybersecurity for remote work.

18.A. Simulation of cyber incidents.

People's lack of attention to cyber threats is often due to a lack of direct experience of significant cyber incidents that have disrupted critical services. A training process that provides employees with direct experience or that simulates a cyber-attack may improve skills and raise awareness.

How important/prioritized do you think it should be to invest in or focus on this action in the future?

- 1 (not important)
- 2 (slightly important)
- 3 (moderately important)
- 4 (important)
- 5 (very important)

18.B. Please indicate any tools and best practices that have already been implemented in your organization, or that you would like to propose for the future, that could be useful for simulating cyber incidents.

19.A. Understanding the limitations of cybersecurity devices

A lack of understanding of cybersecurity devices leads individuals to overestimate the effectiveness of these devices, in providing complete protection and to overlook the need for human oversight. Improving the understanding of such devices will contribute to more effective cybersecurity

management and active oversight.

How important/prioritized do you think it should be to invest in or focus on this action in the future?

- 1 (not important)
- 2 (slightly important)
- 3 (moderately important)
- 4 (important)
- 5 (very important)

19.B. Please indicate any tools and best practices that have already been implemented in your organization, or that you would like to propose for the future, that could be useful to understand the limitations of cybersecurity devices.

20.A. Please propose any other important/prioritized strategies and actions of intervention that, in your experience, it is necessary to invest in and focus on in the future to improve the human role in cybersecurity.

20.B. Please indicate any tools and best practices that have already been implemented in your organization, or that you would like to propose for the future, that could be useful to leverage the additional actions suggested in 20.A.

Appendix B

Delphi Questionnaire – Round 2

Cybersecurity: the key role of humans and possible levers of intervention

As previously announced, our survey is based on the Delphi methodology, which involves two phases of data collection. In the first phase, we gathered your opinions on all the questions and asked you to rate the importance of the identified levers. In this second phase, we will only ask you questions on which there was no consensus among the experts.

We would like to invite you for the second and final time to answer six questions (estimated time: 15 min).

Also, you will find a new question suggested by other experts, on which we are now asking for your opinion.

We are also pleased to provide you with an aggregated and anonymized analysis of the data collected, together with the best practices that have emerged so far, at this [LINK](#).

At the end of the study, we will share the final results with all participants. The objectives of the research are summarized below.

Cybersecurity has become an increasingly important issue for public and private organizations and institutions. In the fight against cyber threats, there is often a tendency to focus on technical factors while neglecting the key role that people play in cybersecurity.

We therefore asked ourselves:

- How can people be a solution (and not a problem) for cybersecurity?
- Is it possible to adopt good management practices, as well as preventive, reactive, and corrective measures that integrate people with technologies and processes?

Traditionally, human factors such as communication, stress, fatigue, and awareness are considered the weakest link in cybersecurity. However, recent studies show that incorporating human factors into cybersecurity is a key step in the development of a holistic approach to the subject. This study, using the Delphi methodology, aims to gather expert opinions and experiences on the importance and implementation of some intervention levers identified in the literature to rethink the human role in cybersecurity.

The results of the study, by integrating theoretical findings from the scientific literature and the opinions of experts in the field, will provide a basis for the development of targeted security strategies, effective training programs, and corporate policies aimed at reducing vulnerabilities and improving the human role in cybersecurity management.

Part 2. Importance of intervention actions

Below are the intervention levers identified in the literature for leveraging human potential for organizational cybersecurity that did not reach consensus in the first round. Looking ahead, please carefully assess each of these levers of intervention on a scale of 1 to 5, indicating how important/prioritized you believe it should be to invest, focus, or concentrate on the business objectives associated with each lever. This assessment will result in a targeted cybersecurity strategy tailored to your organization's specific needs. Given the current business scenario, with often limited resources, it is not always possible to act on every lever, but it is necessary to make judicious choices based on their importance and the resources available.

For each intervention lever, it is therefore necessary to

- Rate its importance from 1 to 5 *.
- Provide any tools and best practices that can be useful to implement it in the future.

At the end of the questionnaire, participants will also have the opportunity to suggest additional intervention levers.

*1 means "not important" and 5 means "very important."

Example of Question 1 proposed for the first statement that did not reach consensus in the first round. The same approach was followed for the other questions.

1.A. Workload balance

The importance of workload management and effective scheduling of activities is emphasized to improve organizational cybersecurity. In situations of high mental stress or intense workload, employees are more likely to make mistakes due to distraction.

From round 1:

Some participants suggested simplifying procedures by finding a balance between security and usability. In order to balance the workload, practices such as adopting biometric authentication as a more user-friendly alternative to cumbersome password requirements or adapting security requirements to one's role could be considered. Some participants argued that this leverage is not specific to cybersecurity activities but applies to all

activities. They emphasized that even when the workload is unbalanced, cybersecurity should remain a priority.

How important/prioritized do you think it should be to invest in or focus on this leverage in the future?

Below is the average value of the answers obtained in the first round +/- their standard deviation. The median value is also shown.



1.B. Please indicate any tools and best practices that have already been implemented in your organization, or that you would like to propose for the future, that could be useful for workload balance.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at [doi:10.1016/j.jik.2025.100695](https://doi.org/10.1016/j.jik.2025.100695).

References

- Abzakh, A., & Althunibat, A. (2023). A review: Human factor and cybersecurity. In *Proceedings of the 2023 international conference on information technology (ICIT)* (pp. 589–592). <https://doi.org/10.1109/ICIT58056.2023.10225828>
- Akter, S., Uddin, M. R., Sajib, S., Lee, W. J. T., Michael, K., & Hossain, M. A. (2022). Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. *Annals of Operations Research*. <https://doi.org/10.1007/s10479-022-04844-8>
- Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. In *Proceedings of the 2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA)* (pp. 1–5). <https://doi.org/10.1109/CyberSA49311.2020.9139638>
- Aljohani, N. R., Aslam, A., Khadidos, A. O., & Hassan, S. U. (2022). Bridging the skill gap between the acquired university curriculum and the requirements of the job market: A data-driven analysis of scientific literature. *Journal of Innovation & Knowledge*, 7 (3), Article 100190. <https://doi.org/10.1016/j.jik.2022.100190>
- Annarelli, A., Colabianchi, S., Nonino, F., & Palombi, G. (2021). The effectiveness of outsourcing cybersecurity practices: a study of the Italian context. *Proceedings of the Future Technologies Conference* (pp. 17–31). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-89912-7_2
- Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of cyber resilient systems. *Computers & Industrial Engineering*, 149, Article 106829. <https://doi.org/10.1016/j.cie.2020.106829>
- Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs. *Decision Support Systems*, 147, Article 113580. <https://doi.org/10.1016/j.dss.2021.113580>
- Avella, J. R. (2016). Delphi panels: Research design, procedures, advantages, and challenges. *International Journal of Doctoral Studies*, 11, 305–321. <https://doi.org/10.28945/3561>. Scopus.
- James Madison University/Louisiana State University/Balozian, P., Burns, A. J., & Leidner, D. E. (2023). An adversarial dance: Toward an understanding of insiders' Responses to organizational information security measures. *Journal of the Association for Information Systems*, 24(1), 161–221. <https://doi.org/10.17705/1jais.00798>
- Bao, Y., Zhu, F., Hu, Y., & Cui, N. (2016). The research of interpersonal conflict and solution strategies. *Psychology*, 07(04), 541–545. <https://doi.org/10.4236/psych.2016.74055>
- Bassanino, M., Fernando, T., & Wu, K. C. (2014). Can virtual workspaces enhance team communication and collaboration in design review meetings? *Architectural Engineering and Design Management*, 10(3–4), 200–217. <https://doi.org/10.1080/17452007.2013.775102>
- Berbel-Vera, J., Barrachina Palanca, M., & Gonzalez-Sanchez, M. B. (2022). Key CDO functions for successful digital transformation: Insights from a Delphi study. *Technological Forecasting and Social Change*, 181, Article 121773. <https://doi.org/10.1016/j.techfore.2022.121773>
- Bergefurt, L., Weijss-Perrée, M., Maris, C., & Appel-Meulenbroek, R. (2021). Analyzing the effects of distractions while working from home on burnout complaints and stress levels among office workers during the COVID-19 pandemic. In *Proceedings of the 3rd international electronic conference on environmental research and public health—public health issues in the context of the COVID-19 pandemic* (p. 44). <https://doi.org/10.3390/ECERPH-3-09075>
- Blair, R. S. (2018). *Introduction to Human Factors and Ergonomics* (4th Edition). Boca Raton, FL, USA: CRC Press.
- Buck, C., Clarke, J., Torres de Oliveira, R., Desouza, K. C., & Maroufkhani, P. (2023). Digital transformation in asset-intensive organisations: The light and the dark side. *Journal of Innovation & Knowledge*, 8(2), Article 100335. <https://doi.org/10.1016/j.jik.2023.100335>
- Carroll, N., Hassan, N. R., Junglas, I., Hess, T., & Morgan, L. (2023). Transform or be transformed: The importance of research on managing and sustaining digital transformations. *European Journal of Information Systems*, 32(3), 347–353. <https://doi.org/10.1080/0960085X.2023.2187033>
- Carroll, J. M. (1997). Human–computer interaction: Psychology as a science of design. *International Journal of Human-Computer Studies*, 46(4), 501–522. <https://doi.org/10.1006/ijhc.1996.0101>
- Cavanaugh, M. A., Boswell, W. R., Roehling, M. V., & Boudreau, J. W. (2000). An empirical examination of self-reported work stress among U.S. managers. *Journal of Applied Psychology*, 85(1), 65–74. <https://doi.org/10.1037/0021-9010.85.1.65>
- Chang, S. I., Chang, L. M., & Liao, J. C. (2020). Risk factors of enterprise internal control under the internet of things governance: A qualitative research approach. *Information & Management*, 57(6), Article 103335. <https://doi.org/10.1016/j.im.2020.103335>
- Checkland, P., & Scholes, J. (1999). *Soft systems methodology in action*. Soft systems methodology in action. Checkland, Peter, Chichester: Wiley (Reprinted).
- Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: Challenges, research focus and recommendations. *IEEE Access : Practical Innovations, Open Solutions*, 1. <https://doi.org/10.1109/ACCESS.2022.3197899>. Scopus.
- Chowdhury, N. H., Adam, M. T. P., & Skinner, G. (2019). The impact of time pressure on cybersecurity behaviour: A systematic literature review. *Behaviour & Information Technology*, 38(12), 1290–1308. <https://doi.org/10.1080/0144929X.2019.1583769>
- Chowdhury, N., Katsikas, S., & Gkioulos, V. (2022). Modeling effective cybersecurity training frameworks: A Delphi method-based study. *Computers & Security*, 113, Article 102551. <https://doi.org/10.1016/j.cose.2021.102551>
- Colabianchi, S., Costantino, F., Di Gravio, G., Nonino, F., & Patriarca, R. (2021). Discussing resilience in the context of cyber physical systems. *Computers & Industrial Engineering*, 160, Article 107534. <https://doi.org/10.1016/j.cie.2021.107534>
- Corrallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Computers in Industry*, 114, Article 103165. <https://doi.org/10.1016/j.compind.2019.103165>
- Corradini, I. (2020a). Security: Human nature and behaviour. In I. Corradini (Ed.), *Building a cybersecurity culture in organizations: 284. Building a cybersecurity culture in organizations* (pp. 23–47). Springer International Publishing. http://link.springer.com/10.1007/978-3-030-43999-6_2
- Corradini, I. (2020b). Security: Human nature and behaviour. In *Building a cybersecurity culture in organizations*, 284 pp. 23–47. Springer International Publishing. http://link.springer.com/10.1007/978-3-030-43999-6_2
- Cost of a data breach Report 2023.(2023). <https://www.ibm.com/reports/data-breach>
- CIEHF. (2022). The role of human factors in delivering cyber security. <https://ergonomics.ics.org.uk/resource/the-role-of-human-factors-in-delivering-cyber-security.html>
- Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, 32, 90–101. <https://doi.org/10.1016/j.cose.2012.09.010>
- D'Arcy, J., Hovav, L., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1), 79–98. <https://doi.org/10.1287/isre.1070.0160>
- Dekker, S., & Hollnagel, E. (2004). Human factors and folk models. *Cognition, Technology & Work*, 6(2), 79–86. <https://doi.org/10.1007/s10111-003-0136-9>
- Demlechner, Q., Schoemer, D., & Laumer, S. (2021). How can artificial intelligence enhance car manufacturing? A Delphi study-based identification and assessment of general use cases. *International Journal of Information Management*, 58. <https://doi.org/10.1016/j.jinfomgt.2021.102317>. Scopus.
- Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2021a). Human Factors in phishing attacks: A systematic literature review. *ACM Computing Surveys*, 54(8). <https://doi.org/10.1145/3469886>, 173:1-173:35.
- Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2021b). Human Factors in phishing attacks: A systematic literature review. *ACM Computing Surveys*, 54(8). <https://doi.org/10.1145/3469886>, 173:1-173:35.
- Dincelli, E., & Chengalur-Smith, I. (2020). Choose your own training adventure: Designing a gamified SETA artefact for improving information security and privacy through interactive storytelling. *European Journal of Information Systems*, 29(6), 669–687. <https://doi.org/10.1080/0960085X.2020.1797546>

- Disconzi, C. M. D. G., & Saurin, T. A. (2022). Design for resilient performance: Concept and principles. *Applied Ergonomics*, 101, Article 103707. <https://doi.org/10.1016/j.apergo.2022.103707>
- Donalds, C., & Osei-Bryson, K. M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management*, 51. <https://doi.org/10.1016/j.ijinfomgt.2019.102056>. Scopus.
- Dupont, G. (2009). Human factors: avoid the dirty dozen with safety nets. *AIR BEAT*. <http://trid.trb.org/view/888331>.
- Edeh, N. C. (2023). Cybersecurity and human factors: A literature review. *Cybersecurity for decision makers* (pp. 45–56). Scopus. https://doi.org/10.1201/9781003319887_3
- Erdogan, G., Romero, A., Zazzeri, N., Zitnik, A., Basile, M., Aprile, G., ... Kechaoglu, I. (2021). Developing cyber-risk centric courses and training material for cyber ranges: A systematic approach. In *Proceedings of the 7th International Conference on Information Systems Security and Privacy*. SciTePress.
- European Digital. (2023). SME Alliance. *Global ransomware landscape*. <https://www.digitalsme.eu/digital/uploads/Report-H2-2023-ENG.pdf>.
- Fard Bahreini, A., Cavusoglu, H., & Cenfetelli, R. T. (2023). How “what you think you know about cybersecurity” can help users make more secure decisions. *Information & Management*, 60(7), Article 103860. <https://doi.org/10.1016/j.im.2023.103860>
- European Union Agency for Network and Information Security. (2018). ENISA threat landscape report 2017. <https://data.europa.eu/doi/10.2824/967192>.
- Ferro, L. S., Marrella, A., Catarci, T., Sapio, F., Parenti, A., & De Santis, M. (2022). AWATO: A serious game to improve cybersecurity awareness. *Lecture notes in computer science* (pp. 508–529). Scopus. https://doi.org/10.1007/978-3-031-05637-6_33 (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 13334 LNCS.
- Foster, C. J., Plant, K. L., & Stanton, N. A. (2020). A Delphi study of human factors methods for the evaluation of adaptation in safety-related organisations. *Safety Science*, 131, Article 104933. <https://doi.org/10.1016/j.ssci.2020.104933>
- Frey, S. (2018). How to eliminate the prevailing ignorance and complacency around cybersecurity (A. c. Di). In M. Bartsch, & S. Frey (Eds.), *Cybersecurity best practices* (pp. 1–10). Fachmedien Wiesbaden: Springer http://link.springer.com/10.1007/978-3-658-21655-9_1.
- Gale, M., Bongiovanni, I., & Slapnicar, S. (2022). Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead. *Computers & Security*, 121, Article 102840. <https://doi.org/10.1016/j.cose.2022.102840>
- Gratian, M., Bandi, S., Kukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers and Security*, 73, 345–358. <https://doi.org/10.1016/j.cose.2017.11.015>. Scopus.
- Henshel, D., Cains, M. G., Hoffman, B., & Kelley, T. (2015). Trust as a Human factor in holistic cyber security risk assessment. *Procedia Manufacturing*, 3, 1117–1124. <https://doi.org/10.1016/j.promfg.2015.07.186>
- Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106–125. <https://doi.org/10.1057/ejis.2009.6>
- Iqbal, M., & Ahmad, M. (2019). Ranking and visualization of experts for communication using LinkedIn (A. c. Di). In K. Arai, R. Bhatia, & S. Kapoor (Eds.), *Proceedings of the future technologies conference (FTC) 2018* (pp. 1–12). Springer International Publishing. https://doi.org/10.1007/978-3-030-02683-7_1.
- Jalali, M. S., Siegel, M., & Madnick, S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *The Journal of Strategic Information Systems*, 28(1), 66–82. <https://doi.org/10.1016/j.jsis.2018.09.003>
- Jayakrishnan, G. C., Banahatti, V., Lodha, S., Sirigireddy, G., & Nivas, S. (2022). Housie: A multiplayer game for cybersecurity training and evaluation. In *Proceedings of the CHI PLAY 2022 - extended abstracts of the 2022 annual symposium on computer-human interaction in play* (pp. 17–23). <https://doi.org/10.1145/3505270.3558328>
- Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019). Towards an improved understanding of human factors in cybersecurity (pp. 338–345). Scopus. <https://doi.org/10.1109/CIC48465.2019.00047>
- Jin, G., Tu, M., Kim, T. H., Heffron, J., & White, J. (2018). Game based cybersecurity training for high school students. In *Proceedings of the 49th ACM technical symposium on computer science education SIGCSE 2018* (pp. 68–73). <https://doi.org/10.1145/3159450.3159591>, 2018-January.
- Kelly, F. E., Frerk, C., Bailey, C. R., Cook, T. M., Ferguson, K., Flin, R., et al. (2023). Implementing human factors in anaesthesia: Guidance for clinicians, departments and hospitals: Guidelines from the difficult airway society and the association of anaesthetists: Guidelines from the difficult airway society and the association of anaesthetists. *Anaesthesia*, 78(4), 458–478. <https://doi.org/10.1111/anae.15941>
- Kompaso, S. M., & Sridevi, M. S. (2010). Employee engagement: The key to improving performance. *International Journal of Business and Management*, 5(12), p89. <https://doi.org/10.5539/ijbm.v5n12p89>
- Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, 25(4), 289–296. <https://doi.org/10.1016/j.cose.2006.02.008>
- Landeta, J., Barrutia, J., & Lertxundi, A. (2011). Hybrid Delphi: A methodology to facilitate contribution from experts in professional contexts. *Technological Forecasting and Social Change*, 78(9), 1629–1641. <https://doi.org/10.1016/j.techfore.2011.03.009>
- Lawshe, C. H. (1975). A quantitative approach to content Validity1. *Personnel Psychology*, 28(4), 563–575. <https://doi.org/10.1111/j.1744-6570.1975.tb01393.x>
- Luoma, P., Penttinen, E., Tapio, P., & Toppinen, A. (2022). Future images of data in circular economy for textiles. *Technological Forecasting and Social Change*, 182, Article 121859. <https://doi.org/10.1016/j.techfore.2022.121859>
- Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, 3(1), 10. <https://doi.org/10.1186/s42400-020-00050-w>
- Mailloux, L. O., Span, M., Mills, R. F., & Young, W. (2019). A top down approach for eliciting systems security requirements for a notional autonomous space system. In *Proceedings of the 2019 IEEE international systems conference (SysCon)* (pp. 1–7). <https://doi.org/10.1109/SYSCON.2019.8836929>
- Majumdar, N., & Ramteke, V. (2022). October). Human elements impacting risky habits in cybersecurity. In , 2519. *AIP Conference Proceedings*. AIP Publishing. 10.1063/5.0110624.
- Malatji, M., Von Solms, S., & Marnewick, A. (2019). Socio-technical systems cybersecurity framework. *Information & Computer Security*, 27(2), 233–272. <https://doi.org/10.1108/ICS-03-2018-0031>
- McIlwraith, A. (2021). *Information security and employee behaviour: how to reduce risk through employee education, training and awareness*. Routledge.
- Miarmi, L., & DeBono, K. G. (2007). The impact of distractions on heuristic processing: Internet advertisements and stereotype use 1. *Journal of Applied Social Psychology*, 37(3), 539–548. <https://doi.org/10.1111/j.1559-1816.2007.00173.x>
- Mitnick, K. D., & Simon, W. L. (2003). *The art of deception: Controlling the human element of security*. John Wiley & Sons.
- Mullen, P. M. (2003). Delphi: Myths and reality. *Journal of Health Organization and Management*, 17(1), 37–52. <https://doi.org/10.1108/1477260310469319>
- Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L. (2012). Exploring game design for cybersecurity training. In *Proceedings of the 2012 IEEE international conference on cyber technology in automation, control, and intelligent systems, CYBER 2012* (pp. 256–262). <https://doi.org/10.1109/CYBER.2012.6392562>
- Nayak, B., Bhattacharyya, S. S., & Krishnamoorthy, B. (2021). Explicating the role of emerging technologies and firm capabilities towards attainment of competitive advantage in health insurance service firms. *Technological Forecasting and Social Change*, 170, Article 120892. <https://doi.org/10.1016/j.techfore.2021.120892>
- Neigel, A. R., Claypoole, V. L., Waldfole, G. E., Acharya, S., & Hancock, G. M. (2020). Holistic cyber hygiene education: Accounting for the human factors. *Computers and Security*, 92. <https://doi.org/10.1016/j.cose.2020.101731>. Scopus.
- NIST. Success stories. (2018). <https://www.nist.gov/cyberframework/success-stories>.
- Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. *HOLISTICA – Journal of Business and Public Administration*, 13(1), 49–72. <https://doi.org/10.2478/hjbpa-2022-0003>
- Norman, K. L. (2017). *Cyberpsychology: An introduction to human-computer interaction* (2nd ed.). Cambridge University Press. <https://doi.org/10.1017/9781316212554>
- Nthala, L., & Flechais, I. (2017). If it's urgent or it is stopping me from doing something, then I might just go straight at it": A study into home data security decisions (A. c. Di). In T. Tryfonas (Ed.), *Human aspects of information security, privacy and trust: 10292. Human aspects of information security, privacy and trust* (pp. 123–142). Springer International Publishing https://link.springer.com/10.1007/978-3-319-58460-7_9.
- Nwankpa, J. K., & Datta, P. M. (2023). Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers. *Computers & Security*, 130, Article 103266. <https://doi.org/10.1016/j.cose.2023.103266>
- Olivares Rojas, J. C., Reyes Archundia, E., Gutierrez Gnechchi, J. A., Mendez Patiño, A., Cerda Jacobo, J., & Molina Moreno, I. (2022). A methodology for cyber hygiene in smart grids. *DYNA*, 97(1), 92–97. <https://doi.org/10.6036/10085>
- Oltramari, A., Henshel, D., Cains, M., & Hoffman, B. (2015). *Towards a human factors ontology for cyber security*. 1523 pp. 26–33. Scopus.
- Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers and Security*, 66, 40–51. <https://doi.org/10.1016/j.cose.2017.01.004>. Scopus.
- Patriarca, R., Falegnami, A., Costantino, F., Di Gravio, G., De Nicola, A., & Villani, M. L. (2021). WAX: An integrated conceptual framework for the analysis of cyber-socio-technical systems. *Safety Science*, 136, Article 105142. <https://doi.org/10.1016/j.ssci.2020.105142>
- Pawlicka, A., Pawlicki, M., Kozik, R., & Choraś, M. (2022). Human-driven and human-centred cybersecurity: Policy-making implications. *Transforming Government: People, Process and Policy*, 16(4), 478–487. <https://doi.org/10.1108/TG-05-2022-0073>. Scopus.
- Pinzone, A., Albè, F., Orlandelli, D., Barletta, I., Berlin, C., Johansson, B., et al. (2020). A framework for operative and social sustainability functionalities in Human-centric cyber-physical production systems. *Computers & Industrial Engineering*, 139, Article 105132. <https://doi.org/10.1016/j.cie.2018.03.028>
- Poller, D. N., Bongiovanni, M., Cochand-Priollet, B., Johnson, S. J., & Perez-Machado, M. (2020). A human factor event-based learning assessment tool for assessment of errors and diagnostic accuracy in histopathology and cytopathology. *Journal of Clinical Pathology*, 73(10), 681–685. <https://doi.org/10.1136/jclinpath-2020-206538>
- Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., et al. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition, Technology & Work*, 24(2), 371–390. <https://doi.org/10.1007/s10111-021-00683-y>
- Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers and Security*, 136. <https://doi.org/10.1016/j.cose.2023.103585>. Scopus.
- Proudfoot, J. G., Cram, W. A., & Madnick, S. (2024). Weathering the storm: Examining how organisations navigate the sea of cybersecurity regulations. *European Journal of Information Systems*, 0(0), 1–24. <https://doi.org/10.1080/0960085X.2024.2345867>
- Rahman, T., Rohan, R., Pal, D., & Kanthamanon, P. (2021). Human factors in cybersecurity: A scoping review. In *Proceedings of the 12th international conference on*

- advances in information technology (pp. 1–11). <https://doi.org/10.1145/3468784.3468789>
- Reeves, A., Calic, D., & Delfabbro, P. (2023). “Generic and unusable”1: Understanding employee perceptions of cybersecurity training and measuring advice fatigue. *Computers & Security*, 128, Article 103137. <https://doi.org/10.1016/j.cose.2023.103137>
- RELX. (2023). Publication of 2023 annual report including financial statements and corporate responsibility report. <https://www.relx.com/media/press-releases/year-2024/annual-report-2023>.
- Röcker, C. (2012). Informal communication and awareness in virtual teams—Why we need smart technologies to support distributed teamwork. *Communications in Information Science and Management Engineering*, 2, 1–15.
- Rogers, K. M., & Ashforth, B. E. (2017). Respect in organizations: Feeling valued as “we” and “me”. *Journal of Management*, 43(5), 1578–1608. <https://doi.org/10.1177/0149206314557159>
- Rowe, G., & Wright, G. (2001). Expert opinions in forecasting: The role of the Delphi technique (A c. Di). In J. S. Armstrong (Ed.), *Principles of forecasting: A handbook for researchers and practitioners* (pp. 125–144). Springer US. https://doi.org/10.1007/978-0-306-47630-3_7
- Sarker, I. H. (2023). Machine learning for intelligent data analysis and automation in cybersecurity: Current and future prospects. *Annals of Data Science*, 10(6), 1473–1498. <https://doi.org/10.1007/s40745-022-00444-2>
- Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J., et al. (2007). Anti-phishing Phil: The design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd symposium on usable privacy and security* (pp. 88–99). <https://doi.org/10.1145/1280680.1280692>
- Sillman, J., Hynynen, K., Dyukov, I., Ahonen, T., & Jalas, M. (2023). Emission reduction targets and electrification of the Finnish energy system with low-carbon power-to-X technologies: Potentials, barriers, and innovations – A Delphi survey. *Technological Forecasting and Social Change*, 193. <https://doi.org/10.1016/j.techfore.2023.122587>. Scopus.
- Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards—A review and comprehensive overview. *Electronics*, 11(14), 2181. <https://doi.org/10.3390/electronics11142181>
- Tejay, G. P. S., & Mohammed, Z. A. (2023). Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective. *Information & Management*, 60(3), Article 103751. <https://doi.org/10.1016/j.im.2022.103751>
- Tiberius, V., Gojowy, R., & Dabić, M. (2022). Forecasting the future of robo advisory: A three-stage Delphi study on economic, technological, and societal implications. *Technological Forecasting and Social Change*, 182, Article 121824. <https://doi.org/10.1016/j.techfore.2022.121824>
- Tonkin, A., Kosasih, W., Grobler, M., & Nasim, M. (2023). Simulating cyber security management: A gamified approach to executive decision making. In *Proceedings of the 37th IEEE/ACM international conference on automated software engineering* (pp. 1–8). <https://doi.org/10.1145/3551349.3561148>
- Triplett, W. J. (2022). Addressing Human factors in cybersecurity leadership. *Journal of Cybersecurity and Privacy*, 2(3), 573–586. <https://doi.org/10.3390/jcp2030029>
- Uebelacker, S., & Quiel, S. (2014). The Social Engineering Personality Framework. In *Proceedings of the 4th workshop on socio-technical aspects in security and trust, STAST 2014 - co-located with 27th IEEE computer security foundations symposium, CSF 2014 in the Vienna summer of logic 2014* (pp. 24–30). <https://doi.org/10.1109/STAST.2014.12>
- Verizon. (2023). 2023 data breach investigations report. Verizon Risk Team. Available: <https://www.verizon.com/business/resources/reports/dbir/>.
- Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE Transactions on Professional Communication*, 55(4), 345–362. <https://doi.org/10.1109/TPC.2012.2208392>
- Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems*, 92, 25–35. <https://doi.org/10.1016/j.dss.2016.09.013>
- Wiegmann, D. A., & Shappell, S. A. (2017). *A human error approach to aviation accident analysis: The human factors analysis and classification system*. Chicago: Routledge.
- Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human Computer Studies*, 120, 1–13. <https://doi.org/10.1016/j.ijhcs.2018.06.004>. Scopus.
- Wong, L. W., Lee, V. H., Tan, G. W. H., Ooi, K. B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, 66. <https://doi.org/10.1016/j.ijinfomgt.2022.102520>. Scopus.
- Young, H., Van Vliet, T., Van De Ven, J., Jol, S., & Broekman, C. (2018). Understanding human factors in cyber security as a dynamic system (A c. Di). In D. Nicholson (Ed.), *Advances in human factors in cybersecurity: 593. Advances in human factors in cybersecurity* (pp. 244–254). Springer International Publishing http://link.springer.com/10.1007/978-3-319-60585-2_23.
- Yukl, G. (2013). *Leadership in organizations* (8th ed.). Pearson. global ed.
- Yusuwan, N. M., Adnan, H., Rashid, Z. Z. A., Ismail, W. N. W., & Mahat, N. A. A. (2021). Towards a successful extension of time (Eot) claim: A consensus view of construction professionals via a modified Delphi method. *Engineering Journal*, 25(1), 263–274. <https://doi.org/10.4186/ej.2021.25.1.263>
- Zarreh, A., Wan, H., Lee, Y., Saygin, C., & Janahi, R. A. (2019). Cybersecurity concerns for total productive maintenance in smart manufacturing systems. *Procedia Manufacturing*, 38, 532–539. <https://doi.org/10.1016/j.promfg.2020.01.067>
- Zimmermann, V., & Renaud, K. (2019). Moving from a ‘human-as-problem’ to a ‘human-as-solution’ cybersecurity mindset. *International Journal of Human-Computer Studies*, 131, 169–187. <https://doi.org/10.1016/j.ijhcs.2019.05.005>