International Journal of Information Security and Privacy
Volume 18 • Issue 1 • January-December 2024

Assessing Employee Susceptibility to Cybersecurity Risks

Rafael Martínez-Peláez
Universidad Católica del Norte, Chile

Pablo Velarde-Alvarado
Universidad Autónoma de Nayarit, Mexico

Vanessa G. Félix
http://orcid.org/0000-0001-9118-8042
Universidad Politécnica de Sinaloa, Mexico & Universidad Autónoma de Occidente, Mexico

Alberto Ochoa-Brust
Universidad de Colima, Mexico

Rodolfo Ostos
https://orcid.org/0000-0003-1429-3660
Universidad Politécnica de Sinaloa, Mexico & Universidad Autónoma de Occidente, Mexico

Luis J. Mena
https://orcid.org/0000-0002-3244-0129
Universidad Politécnica de Sinaloa, Mexico

ABSTRACT

This research challenges assumptions about cybersecurity risk factors, revealing that age, gender, and educational background are not significant determinants of employee susceptibility. It highlights the importance of inclusive cybersecurity training programs that cater to individuals of all age groups, dispelling the misconception that older employees are inherently less tech-savvy and more susceptible to cybersecurity threats. The findings show that cybersecurity teams within organizations significantly impact the adoption of security policies and data handling practices among employees, even though their influence on password and account security practices is limited. Organizations can adopt a holistic approach to cybersecurity training and awareness programs by leveraging these insights. This approach transcends traditional demographics and focuses on enhancing password and account security, ultimately strengthening cybersecurity postures, fostering a culture of cybersecurity consciousness, and fortifying defenses against the evolving landscape of digital threats.

KEYWORDS

Cybersecurity Awareness, Demographics, Human Factors, Privacy Concern, Responsibility

INTRODUCTION

The contemporary business environment relies on information and information systems, exposing organizations to potentially devastating cybersecurity threats (Ogbanufe, 2021; Rahim et al., 2015). Cyberattacks' ramifications are important, from trade secrets to critical system disruptions. A significant driver of these threats is employee noncompliance with information security policies (Alshaikh, 2020; Evans et al., 2016; Khan et al., 2022). To counter this alarming trend, experts emphasize the need to foster cybersecurity awareness and to transform attitudes, perceptions, and practices within organizations (Alshaikh, 2020, Burrell et al., 2020; Chaudhary, 2024; Tjirare & Shava, 2020).

Cybersecurity teams are crucial in defending organizations from cybersecurity threats (Alshaikh, 2020). Their experience strengthens defenses and reduces the risks of infringement (Dalal et al., 2022). However, their impact must go beyond the technical aspects; they must positively influence

DOI: 10.4018/IJISP.359412

employees' cybersecurity awareness to minimize individual and organizational security risks (Klimburg & Wentland, 2021).

Previous studies have analyzed the critical role of cybersecurity teams in safeguarding organizations against the ever-evolving landscape of cyber threats. One notable analysis, the 2019 Ponemon Institute report titled *Cost of a Data Breach Report*, comprehensively analyzed data breaches across various sectors. This report revealed that the average total cost of a data breach amounted to $3.92 million, with the highest financial impacts observed in the healthcare and financial services sectors. The study highlighted a significant finding: the presence of a dedicated cybersecurity team had a substantial cost-reduction effect after a data breach.

Similarly, the 2022 IBM Security X-Force Threat Intelligence Index contributed valuable insights into the temporal aspects of cyberattacks. The report emphasized that organizations with well-established and mature cybersecurity programs demonstrated greater efficiency in detecting and responding to cyber threats than those with less mature programs.

Although previous studies reviewed the influence of organizational factors on cybersecurity posture, we have identified a significant gap in research on how the presence of cybersecurity teams directly influences the reduction of employee risk levels. Furthermore, the current literature offers few details on the correlation among demographic factors, such as age, gender, and educational level, and the presence of cybersecurity teams on employees' susceptibility to cybersecurity risks. This research gap led us to define the following research question: How do different demographic factors (such as age, gender, and educational level) and the presence of cybersecurity teams in organizations influence employees' susceptibility to cybersecurity risks?

This study explores two critical ways cybersecurity teams can impact organizational security posture: a) raise employee awareness of cybersecurity and b) improve employee adherence to security policies. By focusing on these two areas, we seek not only to evaluate the tangible results of cybersecurity teams' efforts, but also to understand how specific demographic factors, cultural intelligence and social capital can influence the effectiveness of those efforts. Cultural intelligence enhances employees' ability to engage with and adapt to diverse cybersecurity challenges, while social capital fosters collaboration and knowledge sharing within the organization. These factors are instrumental in amplifying the impact of cybersecurity teams by promoting a culture of inclusivity, engagement, and mutual support. We aim to address a crucial gap in the existing literature and provide new insights into how cybersecurity teamscan strengthen organizational security posture, focusing on employee awareness.

BACKGROUND

Cultural Intelligence

Cultural intelligence has become essential for an increasingly globalized society, especially in the technological field, where personnel move between different social, economic, and cultural contexts (Li et al., 2016). This consist in the ability of people to adapt to and interact effectively with people from diverse cultural backgrounds (Crowne, 2008). This ability is not limited to specific cultures but involves managing emotions and physical presence (Schühly, 2022). People with high cultural intelligence can better confront global cyber threats in cybersecurity, adapting their security practices to different cultural environments (Ogbanufe, 2021). Thus, is a valuable resource for success in the context of cybersecurity culture (Cabral et al., 2020; Ponemon Institute, 2019).

Cybersecurity Awareness

Cybersecurity awareness is essential for the ability of individuals, organizations, and nations to recognize and respond to digital threats (Chaudhary, 2024; Khan et al., 2022). This concept involves educating users about online risks, such as fraud and malware attacks, and promoting safe practices

in the digital space (Evans et al., 2016; Khan et al., 2022). Because of the increasing incidence of cybercrimes around the world, it is crucial that cybersecurity training become more widespread (Martins & Medeiros, 2022). Awareness allows people to identify threats and proactively protect their information and digital assets, becoming the first defense against cyberattacks (Georgiadou et al., 2021a).

For that reason, cybersecurity awareness has become an element of national security in today's interconnected world (Onumo et al., 2021; Safi & Browne, 2023). The rising tide of cybercrimes, data breaches, and cyberattacks poses significant challenges to governments and organizations worldwide (Martins & Medeiros, 2022).

Cybersecurity Risk Perception

Cybersecurity is a field characterized by constant digital threats and potential vulnerabilities (Pollini et al., 2022). To comprehend how individuals perceive and respond to these risks, a fusion of diverse theories offers a comprehensive lens that illuminates the multidimensional nature of cybersecurity risk perception (Khan et al., 2022; Safa et al., 2015; Tsohou et al., 2015).

Examining age, gender, and education disparities deepens our understanding of how different demographic groups evaluate risks in the digital age (Georgiadou et al., 2021b; Klimburg & Wentland, 2021). Integrating insights into these disparities and normative influences allows us to construct a more enriched understanding of how individuals confront digital risks. As cyberattacks evolve, the balance between emotional reactions and analytical assessments shapes people's responses to cyber threats (Thangavelu et al., 2021; Tsohou et al., 2015).

Emotions evoked by affect-driven methods, such as the fear of data breaches, often converge with analytical assessments based on past experiences and normative influences (Dalal et al., 2022). This dynamic interaction between emotional and logical responses is crucial in determining how individuals perceive and respond to cyber threats.

Social Capital

Social capital is a concept that underscores the significance of social interactions and the value derived from connections, relationships, and networks within various settings. Social capital is crucial at different levels in facilitating access to resources, information, and support (Seibert et al., 2001).

At the individual level, social capital encompasses the personal relationships and networks a person builds, enabling them to tap into valuable resources, information, and support. These connections can prove instrumental in personal and professional growth, allowing individuals to expand their knowledge and access critical resources (Kam et al., 2020; Kim & Canella, 2008;

At the community level, social capital thrives within community members' social connections and networks. These ties foster trust, cooperation, and collective action within the community, encouraging members to work together toward common goals (Ahmad et al. 2020). Consequently, communities can effectively address shared challenges and make joint decisions that benefit all.

Within an organization, social capital forms relationships and networks among its employees or members. This internal social capital enhances team members' collaboration, communication, and knowledge sharing (Amankwa et al., 2021). Therefore, a culture of openness and information sharing allows organizations to harness the collective intelligence of their workforce, leading to more significant innovation and problem solving capabilities.

The relevance of social capital lies in its power to facilitate cooperation, trust, and reciprocity between individuals and groups, fostering social connections at various levels within organizations to build effective collaboration and shared success.

In the context of cybersecurity leadership, social capital gains even more significance. Building and leveraging personal networks enables cybersecurity professionals to access essential information, resources, and expertise swiftly (Seibert et al., 2001). This advantage is particularly crucial in

cybersecurity, where rapid responses to emerging threats are critical to maintaining a robust security posture (Dalal et al., 2022).

Likewise, forging connections with other cybersecurity experts and organizations at the community level fosters a collective effort to combat cyber threats (Chaudhary, 2024). Thus, communities of cybersecurity practitioners can enhance their ability to anticipate and respond to cyberattacks, effectively pooling knowledge and resources against malicious users.

Within an organization, social capital among employees strengthens teamwork and cooperation. When employees feel comfortable sharing information and ideas, it leads to a more comprehensive understanding of potential risks and vulnerabilities. This collaborative culture contributes to a more robust cybersecurity strategy and proactive measures to safeguard sensitive data and systems (Renaud et al., 2019).

Therefore, social capital is a powerful catalyst for effective collaboration and information sharing among individuals, communities, and organizations. Emphasizing the value of personal connections, community cooperation, and internal networks can significantly bolster cybersecurity efforts and overall organizational performance (Rodgers et al., 2019). By recognizing and harnessing the potential of social capital, leaders can build resilient cybersecurity cultures and foster a united front against ever-evolving cyber threats (Flores & Ekstedt, 2016).

Cybersecurity Culture in Organizations

Cybersecurity culture is a critical aspect of organizational security, involving the development of shared understanding, beliefs, attitudes, and behaviors among employees to protect information assets from cyber threats (Pollini et al., 2022). This culture safeguards cyberspace, organizational data, and consumers from potential cyberattacks, combining corporate and individual security factors by assessing security policies and procedures as they relate to employees' behaviors, attitudes, and skills (Gioulekas et al. 2022).

Cybersecurity culture has gained significant attention in recent years, with various research studies emphasizing its importance for organizational security (Georgiadou et al., 2021a). For instance, the European Union's Energy Shield project introduced a Cybersecurity Culture Framework in 2020 to assess individuals' and organizations' readiness for security culture (Georgiadou et al., 2022b. This framework employs evaluation techniques to effectively gauge security metrics, including surveys, tests, simulations, and serious games.

Building an influential cybersecurity culture requires regular communication, awareness, training, and education initiatives to ensure that all employees thoroughly understand the organization's security policies and implement them cautiously (Ahmad et al., 2020). This approach helps prevent security breaches resulting from noncompliance with security policies and provides information security seamlessly integrated into daily activities (Hasan et al., 2021).

Organizations must take a holistic approach to achieve a robust cybersecurity culture that addresses people, processes, and technology (Berlilana et al., 2021). Beyond merely providing annual security training, a broader strategy that instills transformative changes in attitudes, perceptions, routines, assumptions, and new skills is essential. Additionally, management support plays a significant role, providing legal guarantees for access to necessary information and resources and ensuring the availability of required education and information technologies products (Georgiadou et al., 2022a).

Organizational culture also plays a vital role in shaping cybersecurity culture, and the two are inherently interconnected. Cybersecurity culture should be woven into employee work, habits, and behavior, making it an essential component of the overall organizational culture (Georgiadou et al., 2022a). Creating a security culture that encourages employees to be proactive in identifying and mitigating cyber threats is crucial, promoting a sense of responsibility for cybersecurity across all levels of the organization (Kweon et al., 2021).

Cybersecurity culture is a collective effort, aligning organizational security policies with individual behaviors and attitudes. By fostering a culture of embracing cybersecurity as everyone's

responsibility, organizations can effectively safeguard their information assets and enhance their cybersecurity resilience against potential threats (Dalal et al., 2022). This proactive commitment to cybersecurity creates a robust defense against evolving cyber risks, contributing to the long-term success and security of the organization.

RESEARCH METHODOLOGY

This research proposes to help better understand relationships between several demographic and organizational variables, including age, gender, education, and the presence of a cybersecurity team to know the employees' risk levels. Importantly, it delves into the influence of cybersecurity teams on critical aspects of cybersecurity, explicitly focusing on password and account security practices, adherence to security policies, and the depth of computer security awareness (Erendor & Yildirim, 2022; Pratama et al., 2022).

This investigation explored the associations between risk levels and various demographic and security-related variables, including age, gender, education, the presence of a cybersecurity team, password and account security practices, security policies and data handling, and computer security and awareness. By understanding these associations, the study aims to inform cybersecurity strategies and interventions to manage and reduce risk within the organization effectively.

Survey Instrument

A valuable tool to assess an organization's security awareness programs is the Employee Security Awareness Survey (Bond, 2012). We thoughtfully used this survey for employees, enabling them to respond on the basis of their knowledge and understanding of security practices. The instrument used to collect the data has been widely recognized in the field of information security. It was developed by Trenton Bond and supported by SANS Education, one of the leading institutions in cybersecurity training and certification. Similar studies have verified its validity and applicability, providing an additional layer of credibility and robustness to the results obtained. Utilizing this established tool ensured that the survey effectively measured employees' awareness and compliance with security policies, offering reliable insights into the organization's cybersecurity posture.

In addition to categorizing organizations according to risk scores, we also developed risk levels to categorize individuals, ensuring a comprehensive analysis of organizational and individual security awareness. This categorization aims to identify not only an organization's vision but also the individual's vision in terms of cybersecurity awareness.

The survey consists of 24 questions (see Appendix); however, only 23 questions contribute to computing the employees' risk level. Each question is thoughtfully assigned a risk value (ranging from 1 to 5) according to the employees' responses. Higher risk values indicate weaker awareness, negligent behaviors, or engagement in high-risk activities. On the other hand, lower-risk values signify strong security awareness and commitment to best practices.

The risk levels categorize individuals according to their low- to high-risk scores. A lower score indicates that users know sound security principles and threats, comply with organizational security standards, and receive proper training. On the other hand, a higher score suggests a lack of security awareness and adherence to corporate policies, increasing the risk of security incidents.

We incorporated six additional questions to obtain demographic data from the participants. These demographic questions provided us with a comprehensive understanding of the respondents' backgrounds and contexts, enabling us to analyze further the correlations with individuals' risk levels.

Risk Level Calculation

To calculate the individual's risk score for each survey participant, we utilized the following equation, where X represents the numerical value associated with the response to each of the 24 questions based on survey instrument:

Table 1. Individual's risk level

Risk Level	*Range*	*Value*
Low	25 *to* 41	1
Moderate	42 *to* 58	2
Elevated	59 *to* 75	3
Significant	76 *to* 92	4
High	93 *to* 110	5

$$IRS = \sum_{i=2}^{25} X_i$$

The risk level is subsequently determined by referring to Table 1.

Research Model

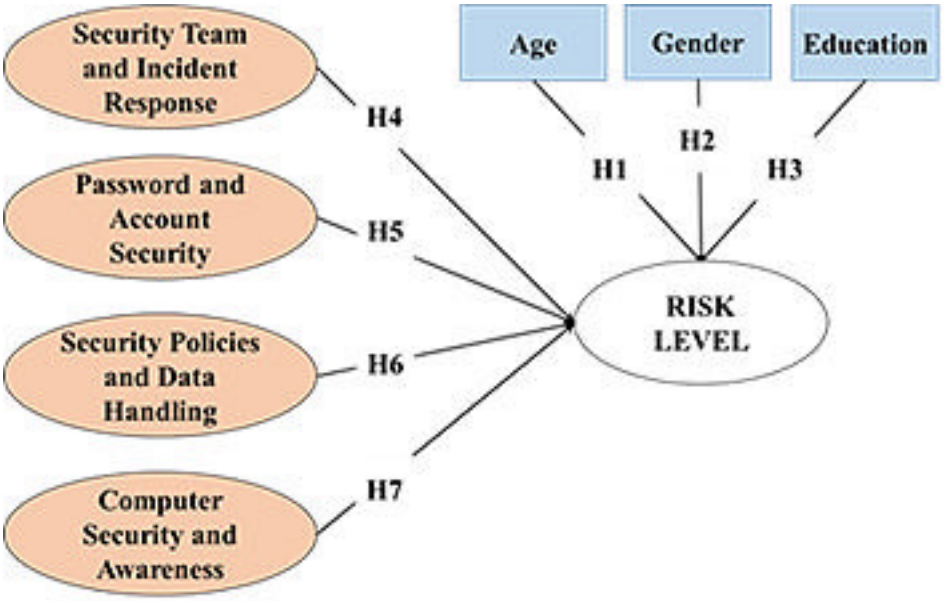
The 24 questions in the Employee Security Awareness Survey have been organized into four groups to comprehensively assess the organization's security posture and employee awareness (see Appendix). The justification for creating these groups is based on the specific focus and thematic coherence of each set of questions. The groups are as follows:

1. The Security Team and Incident Response questions (Group 1; G1) pertain to an organization's cybersecurity team's presence, effectiveness, and preparedness to respond to potential security incidents. Understanding the existence and functionality of a dedicated cybersecurity team is crucial to gauging the level of immediate support available in handling security-related issues.
2. The Computer Security and Awareness questions (Group 2; G2) focus on employees' knowledge and awareness of computer security best practices. Questions in this category aim to assess how well-informed a workforce is about identifying threats, recognizing signs of compromise, and utilizing essential security measures like firewalls, anti-virus software, and regular software updates.
3. The Password and Account Security questions (Group 3; G3) concern account security, which is critical to overall cybersecurity. This group of questions concentrates on employees' password practices, the potential risks associated with password sharing, and the extent to which personal and work account passwords are kept separate.
4. The Security Policies and Data Handling questions (Group 4; G4) concern security policies, which form the foundation of our cybersecurity framework. Questions in this group explore employees' familiarity with organizational policies regarding website access, email usage, instant messaging, and handling sensitive data. Understanding adherence to these policies is crucial for safeguarding confidential information.

In this research, the concept of risk level refers to the level of risk or vulnerability an individual or organization faces concerning cybersecurity threats. It often considers various factors, such as the types of data or assets that need protection, the potential dangers or vulnerabilities, and the potential impact of a security breach. Risk level assessment is a crucial component of cybersecurity management, and it informs decisions about security measures and investments. Figure 1 shows the research model used in this study.

The research model aimed to comprehensively understand the factors influencing employees' cybersecurity risk levels within an organization, facilitating data-driven decisions to enhance the cybersecurity posture.

Figure 1. Research model structure



Cybersecurity Risk Perception in the Model

Currently, the importance of cybersecurity cannot be overstated. As businesses and organizations increasingly rely on technology to function efficiently, they become more vulnerable to cyber threats. It is crucial to comprehend how individuals perceive cybersecurity risks, as their awareness and actions play a pivotal role in safeguarding sensitive data and systems.

One of the intriguing aspects of cybersecurity risk perception is how it varies with age. It is natural to assume that younger employees, who have grown up in a digital world, might be more attuned to cyber risks. However, age can also bring experience and knowledge, contributing to a more nuanced understanding of cybersecurity. Understanding this association between age and risk perception is essential for tailoring cybersecurity awareness programs to different age groups (Rahim et al., 2015). We thus propose

H1: There is a significant correlation between the level of cyber risk and the age of employees.

Cyber risk perception can vary across age groups, as younger employees may be more familiar with technology. In comparison, older employees may bring experience and a deeper understanding of cyber threats.

Gender diversity in the workplace extends to cybersecurity risk perception. Research suggests that men and women perceive cybersecurity risks differently. Examining this association can uncover valuable insights into the factors that shape risk perception. For example, it might reveal whether specific gender-related experiences or biases influence how employees perceive and respond to cyber threats (Georgiadou et al., 2023). We thus propose

H2: There is a significant correlation between the level of cyber risk and employees' gender.

Differences in cyber risk perception between men and women are anticipated to manifest significantly; these differences may be influenced by gender-related experiences and biases that affect how each group perceives and responds to cyber threats.

Education undoubtedly plays a vital role in shaping cybersecurity awareness. Employees with higher levels of education may have a deeper understanding of cyber risks and security practices. However, formal education is not the only important factor at play; another factor is the presence

of ongoing organizational training and awareness programs. Exploring this association helps organizations tailor their cybersecurity education efforts to match the educational backgrounds of their employees (Georgiadou et al., 2021b). We thus propose

H3: There is a significant correlation between the level of cyber risk and the educational level of employees. It is postulated that employees with a higher level of education, including formal training and ongoing cybersecurity training programs, will have a more robust understanding of cyber risks and security practices, which will positively influence their risk perception.

By investigating the associations between age, gender, education, and risk perception, organizations can design targeted awareness campaigns and training programs that empower employees to protect against cyber threats actively.

Cultural Intelligence in the Model

Cultural intelligence comprises several components that enable people to navigate cross-cultural interactions effectively. These include cultural knowledge, mindfulness, and behavioral skills. By mastering these components, people can improve their understanding of cultural differences, leading to more successful interactions. Cultural intelligence also involves the motivation to learn about and adapt to new cultural contexts, including cybersecurity (Alamman et al., 2022; Flores & Ekstedt, 2016). We thus propose

H4: The presence of cybersecurity teams is positively correlated with employees' cyber risk level. The training and support provided by cybersecurity teams are expected to contribute to a greater understanding and mitigation of cyber risks among employees, resulting in a lower overall risk level.

The positive correlation between the presence of a cybersecurity team and employees' overall risk level emphasizes the importance of cultural intelligence in cybersecurity. An organization that values cultural intelligence recognizes that cybersecurity is not solely a technical matter but one deeply interlaced with human behavior, cultural norms, and global perspectives.

Cybersecurity Awareness in the Model

Cybersecurity awareness is a multifaceted concept with far-reaching implications, particularly in cybersecurity. It involves comprehending the activities, events, and risks surrounding individuals and providing context for their actions. In today's interconnected world, cybersecurity awareness is not just a luxury but a necessity. It equips individuals, organizations, and even nations with the knowledge and insights required to identify and respond effectively to the myriad cyber threats and vulnerabilities that pervade the digital landscape.

The following hypothesis suggests that individuals who follow the best password management and account security practices contribute positively to an organization's overall cybersecurity awareness. When employees actively engage in secure practices, they set an example for their peers and demonstrate the importance of cybersecurity, fostering a culture of vigilance and awareness where everyone is more attuned to potential threats and risks (Pratama et al., 2022).

H5: Strong password management and account security practices are associated with lower employee risk levels. It is postulated that employees who adopt appropriate security practices for password and account management not only reduce their risk level but also serve as role models, promoting a more robust organizational cybersecurity culture.

The following hypothesis underscores the significance of organizational security policies and responsible data handling in promoting cybersecurity awareness. When employees adhere to security policies and handle data responsibly, they reinforce the importance of these measures and contribute to a collective understanding of the organization's commitment to cybersecurity. Consequently, this adherence nurtures a culture where cybersecurity awareness is a shared value and employees are more likely to be aware of and compliant with security protocols (Martins & Medeiros, 2022; Ogbanufe, 2021).

H6: Adherence to security policies and responsible data handling are associated with lower employee risk levels. Compliance with security policies and responsible data handling practices are expected to foster an environment where cybersecurity awareness is valued and maintained, contributing to an overall decrease in employee cyber risk.

The following hypothesis highlights the role of computer security knowledge and general awareness in enhancing overall awareness levels. Employees who have a solid understanding of computer security concepts and who stay informed about evolving threats play a crucial role in promoting awareness. Their knowledge is shared with colleagues, creating a collective awareness and a more knowledgeable workforce, strengthening the organization's cybersecurity posture by ensuring that employees are well prepared to identify and respond to potential risks (Kam et al., 2020).

H7: Cybersecurity knowledge and general awareness are associated with lower employee risk levels. Employees with a solid understanding of cybersecurity concepts and an awareness of evolving threats are theorized to be critical in improving organizational cybersecurity awareness, resulting in a more prepared workforce and less vulnerability to cyber risks.

Understanding these practices equips employees with the tools to recognize potential hazards, enhancing their overall cyber threat detection skills. This alignment fosters a culture of proactive security vigilance and empowers individuals to respond effectively to emerging cyber threats.

Social Capital in the Model

Social capital forms a powerful catalyst for fostering effective collaboration, sharing information, and bolstering organizational cybersecurity efforts.

At its core, social capital becomes an internal force within an organization, shaping relationships and networks among employees or members (Rodgers et al., 2019). This internal social capital is a foundation for enhanced collaboration, communication, and knowledge sharing. Through cultivating a culture of openness and information exchange, organizations harness the collective intelligence of their workforce, leading to more significant innovation and problem solving capabilities.

Cybersecurity professionals, by building and leveraging personal networks, gain access to essential information, resources, and expertise. This advantage proves crucial in a field where rapid responses to emerging threats are pivotal in maintaining a robust security posture. Furthermore, forging connections with fellow cybersecurity experts and organizations on a broader scale cultivates a united front against cyber threats (Thangavelu et al., 2021; Kam et al., 2020; Pratama et al., 2022). By pooling knowledge and resources, these communities of practitioners strengthen their ability to anticipate and effectively respond to cyberattacks.

H8: The presence of security teams in an organization positively influences employees' awareness of computer security and response capacity. It is postulated that the interaction and support provided by security teams foster greater awareness among employees about cybersecurity practices, resulting in a more robust organizational culture.

H9: The presence of security teams in an organization positively influences employees' proper management of passwords and account security. Through training and leadership, security teams are expected to improve employee password management and account security practices, contributing to the organization's cyber risk reduction.

H10: The presence of security teams in an organization positively influences the adoption of security policies and the responsible management of data among employees. It is theorized that security teams' intervention will promote greater adherence to established security policies and best practices in data handling, thereby strengthening an organization's overall cybersecurity posture.

Social capital has a profound impact even within an organization's daily operations. Employees who feel at ease sharing information and ideas contribute to a comprehensive understanding of potential risks and vulnerabilities. This culture of collaboration feeds into a more resilient cybersecurity strategy, leading to proactive measures to safeguard sensitive data and systems.

Table 2. Descriptive statistics

Item	*Mean*	*SD*	*Kurtosis*	*Shapiro-Wilk*	*P-Value*
Q2	2.282	1.415	-1.87	0.686	<0.001
Q3	2.018	1.75	-0.708	0.542	<0.001
Q4	2.782	0.98	-1.828	0.619	<0.001
Q5	2.064	1.442	-1.65	0.605	<0.001
Q6	1.509	1.339	-.3201	0.391	<0.001
Q7	2.445	1.506	-2.032	0.636	<0.001
Q8	1.727	1.196	-0.54	0.6	<0.001
Q9	1.8	1.501	0.122	0.544	<0.001
Q10	2.164	1.784	-1.093	0.594	<0.001
Q11	1.818	0.988	-1.894	0.624	<0.001
Q12	2.2	1.841	-1.24	0.575	<0.001
Q13	1.691	1.519	1.102	0.457	<0.001
Q14	1.6	1.416	1.945	0.437	<0.001
Q15	1.436	1.253	4.547	0.36	<0.001
Q16	2.455	1.282	-1.675	0.762	<0.001
Q17	2.391	1.348	-1.766	0.736	<0.001
Q18	1.1	0.301	5.408	0.342	<0.001
Q19	3.327	1.853	-1.839	0.7	<0.001
Q20	1.609	0.49	-1.828	0.619	<0.001
Q21	1.327	0.94	4.547	0.36	<0.001
Q22	1.627	1.226	0.106	0.499	<0.001
Q23	2.8	1.749	-1.775	0.764	<0.001
Q24	1.518	1.139	1.102	0.457	<0.001
Q25	1.818	1.342	-0.947	0.556	<0.001

Data Collected

The data collection period was from November 1, 2022, to November 30, 2022. Out of the 150 employees invited to participate, 110 individuals visited the Google form and completed the online survey. The analysis in the following paragraphs includes the responses from the 110 participants who completed the study.

RESULTS

Descriptive Analysis

The descriptive statistics of the survey data, as presented in Table 2, provide valuable insights into the distribution and characteristics of each survey item. Each item's mean (average) and standard deviation (SD) give an overview OF the central tendency and variability in participants' responses.

We present a detailed interpretation of the findings for each group.

Questions in G1 sought to gauge participants' awareness of the existence of a cybersecurity team within the organization. The mean score for this question was approximately 2.282, indicating

moderate awareness among respondents. The significant departure from normality ($P < 0.001$) suggests a non-uniform distribution of responses.

Questions in G2 included questions concerning various aspects of computer security and awareness. Mean scores ranged from 1.327 to 3.327, reflecting varying levels of understanding and practice. For instance, Q10 demonstrated higher mean scores, indicating more vital awareness. However, all questions within this group significantly deviated from normality ($P < 0.001$), indicating non-normally distributed responses.

Questions in G3 investigated employees' practices related to password and account security (Q6, Q21, Q22). The mean scores ranged from 1.509 to 2.2, signifying different levels of security practices. The kurtosis values varied, suggesting variations in response distributions. Similar to the previous groups, questions in this category significantly deviated from normality ($P < 0.001$).

In the questions in G4, mean scores ranged from 1.1 to 2.8, highlighting diverse perceptions and behaviors. *Q19* had the highest mean score, indicating potentially more vital adherence to data security policies. Notably, all questions in this group exhibited significant deviations from normality ($P < 0.001$).

Our analysis of the risk level in cybersecurity survey data revealed variations in respondents' awareness, practices, and attitudes across different cybersecurity-related groups. The non-normality of the data emphasizes the importance of employing non-parametric statistical methods for further analysis. These findings provide valuable insights into the current state of cybersecurity awareness and practices among the surveyed employees.

Reliability

Reliability tests of the survey data, as presented in Table 3, demonstrate a satisfactory level of internal consistency for the survey instrument, with a McDonald's $\omega = 0.732$ and Cronbach $\alpha = 0.722$. The ω and α values indicate that the survey items consistently measure the constructs of interest, ensuring the stability of the responses obtained across different subsets of questions. The value of McDonald's ω, above the threshold of 0.70, reinforces the idea that the questionnaire's structure is robust and suitable for measuring the critical dimensions of employee safety awareness. Similarly, the comparable Cronbach α coefficient indicates that the responses tend to be consistent, minimizing the possibility of obtaining erratic or incongruent results. These levels of reliability are essential to ensuring that the conclusions derived from the study adequately reflect the attitudes and behaviors of employees towards cybersecurity. In the context of the current research, these reliability indicators allow us to confidently state that the survey instrument used is adequate to capture the variability in employee security awareness linked to demographic factors and cybersecurity equipment. Thus, the study results are consistent and reproducible measurements, strengthening the validity of the inferences of these factors on the organizational security posture.

The values of McDonald's ω and Cronbach's α provide an additional perspective on the internal consistency of the items. These coefficients are in the range from 0.681 to 0.738, indicating a generally acceptable level of internal reliability.

Risk Level

The individual risk level assessment results provide a comprehensive view of the cybersecurity risk landscape among the surveyed individuals. The individual's risk level contains five distinct levels, each providing insight into the different levels of susceptibility to cybersecurity threats. Figure 2 shows the results of our analysis in terms of risk level.

In the analysis of the survey participants, we identified four distinct risk categories. The Low Risk category comprises 36 individuals with a relatively lower susceptibility to cybersecurity threats. Even within this group, maintaining security awareness is essential to preventing complacency in their cybersecurity practices. The Moderate Risk category, which was the most substantial, with 50

Table 3. Reliability statistics

Frequentist Scale Reliability Statistics		
Estimate	*McDonald's ω*	*Cronbach's α*
Point estimate	0.732	0.722
Frequentist individual item reliability statistics		
Item	***McDonald's ω***	***Cronbach's α***
Q2	0.701	0.702
Q3	0.717	0.705
Q4	0.731	0.722
Q5	0.722	0.709
Q6	0.728	0.714
Q7	0.738	0.727
Q8	0.734	0.725
Q9	0.705	0.728
Q10	0.738	0.71
Q11	0.721	0.694
Q12	0.682	0.694
Q13	0.703	0.698
Q14	0.732	0.721
Q15	0.722	0.71
Q16	0.711	0.708
Q17	0.701	0.702
Q18	0.732	0.723
Q19	0.697	0.699
Q20	0.733	0.723
Q21	0.729	0.718
Q22	0.728	0.719
Q23	0.731	0.72
Q24	0.728	0.715
Q25	0.731	0.719

participants, shows a reasonable level of risk and underscores the need for tailored cybersecurity efforts to address the diverse needs of this segment.

The Elevated Risk group, consisting of 23 individuals, is more susceptible to cybersecurity threats. Finally, in the Significant Risk category, only one individual faces an exceptionally high level of cybersecurity risk. This situation demands immediate and intensive attention to address and mitigate potential threats effectively. These categorizations reveal the varying degrees of vulnerability to cybersecurity threats within the surveyed population, emphasizing the necessity of a nuanced and adaptive approach to cybersecurity measures.

Figure 2. Individual's risk levels

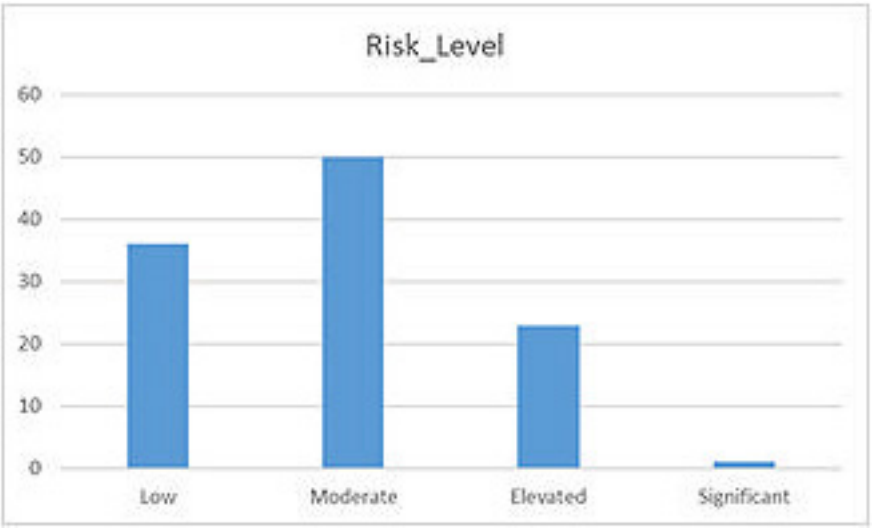


Table 4. Association analysis

Relationships	*Chi-Squared Value*	*Degree of Freedom*	*P-Value*
RISK_LEVEL – AGE	18.369	12	0.105
RISK_LEVEL – GENDER	7.113	6	0.311
RISK_LEVEL – EDUCATION	7.948	6	0.242
RISK_LEVEL – G1	22.061	6	0.001
RISK_LEVEL – G2	208.618	81	<0.001
RISK_LEVEL – G3	33.065	15	0.005
RISK_LEVEL – G4	122.762	66	<0.001
G1 – G2	73.646	54	0.039
G1 – G3	5.836	10	0.829
G1 – G4	52.353	44	0.181

Measurement Model

Our analytical framework began with association analysis, leveraging chi-square tests to identify intricate connections between variables. This approach is justified, since chi-square tests are particularly suitable for evaluating the relationship between categorical variables, allowing one to determine whether a significant association exists without assuming the normality of the data. Our study analyses the relationship between the cyber risk level (*RISK_LEVEL*) and categorical demographic and behavioral variables such as age, gender, education and specific behavior in the work environment (G1, G2, G3 and G4). Subsequently, our exploration included the correlation analysis to illuminate the nature of the relationships within the data. This integrated approach provided a comprehensive view of the complexities and relationships in the data, enriching our understanding of the factors that influence susceptibility to cyber risks. Table 4 presents the association analysis results between the RISK_LEVEL variable and several other variables, including AGE, GENDER, EDUCATION, and the groups G1, G2, G3, and G4.

The first relationship (RISK_LEVEL - AGE) shows a Chi-squared value of 18.369 with 12 degrees of freedom and a *P*-value of 0.105, suggesting that there is no significant association between the risk level and the age of employees, as the *P-value* is more significant than 0.05. In other words, employees' age does not appear significantly related to their cybersecurity risk level.

The second relationship (RISK_LEVEL - GENDER) shows a Chi-squared value of 7.113 with 6 degrees of freedom and a *P*-value of 0.311, indicating that there is no significant association between the risk level and the gender of employees, as the *P*-value is more significant than 0.05. In summary, employees' gender does not seem significantly related to their cybersecurity risk level.

The third relationships (RISK_LEVEL - EDUCATION) reveals a Chi-squared value of 7.948 with 6 degrees of freedom and a *P*-value of 0.242, suggesting that there is no significant association between the risk level and the education level of employees, as the *P*-value is more significant than 0.05. In other words, employees' education level is not significantly related to their cybersecurity risk level.

However, the relations (RISK_LEVEL - G1, G2, G3, G4) concern to specific characteristics or behaviors related to cybersecurity in the workplace. The analyses show significantly high Chi-squared values (22.061, 83.157, 32.366, and 81.852, respectively), with very low *P*-values (< 0.001 in all cases), indicating a significant association between the risk level and these variables. In other words, the results suggest that certain specific behaviors or characteristics in the cybersecurity environment, represented by G1, G2, G3, and G4, are strongly associated with the risk level of employees.

When examining the relationship between behaviors categorized under G1 (such as cybersecurity team presence) and G2 (related to computer security and awareness), the Chi-squared value is 73.643, with 54 degrees of freedom and a *P-value* of 0.039, indicating a significant association between these aspects. In simpler terms, a cybersecurity team correlates strongly with employees' computer security awareness.

The analysis of the relationship between G1 and G3 (about password and account security) shows a Chi-squared value of 5.836, with 10 degrees of freedom and a *P*-value of 0.829. The *P*-value is much greater than 0.05, indicating no significant association. In essence, the presence of a cybersecurity team is not significantly related to password and account security practices.

Finally, when examining the relationship between G1 and G4 (which involves security policies and data handling), the Chi-squared value is 52.353, with 44 degrees of freedom and a *P*-value of 0.181. Similar to G3, this relationship also lacks significant association. Hence, the presence of a cybersecurity team is not significantly related to adherence to security policies and data handling.

The results of this association analysis indicate that while age, gender, and education level do not appear to be significantly related to the cybersecurity risk level, certain behaviors or characteristics in the cybersecurity environment, represented by G1, G2, G3, and G4, have a strong association with the risk level perceived by employees. The presence of a cybersecurity team notably influences computer security awareness; however, the presence of a cybersecurity team has little impact on password and account security practices or adherence to security policies and data handling. These insights can guide organizations in tailoring their cybersecurity strategies to enhance awareness and procedures effectively.

Table 5 shows the results of correlation analyses between the RISK_LEVEL variable and several other variables, including AGE, GENDER, EDUCATION, and the variables G1, G2, G3, and G4. We used Spearman´s and Kendall´s correlation methods (Puth et al., 2015) to assess these relationships.

The results suggest that age and gender have no significant correlation with employees' perceived risk level in cybersecurity. However, a significant negative correlation exists between education level and risk level, implying that higher education is associated with a lower perceived cybersecurity risk level. Furthermore, the variables G1, G2, G3, and G4 show strong positive correlations with the risk level, indicating that specific cybersecurity behaviors and characteristics represented by these variables are closely related to employees' perceived risk levels.

Table 5. Correlation analysis

Relationships	*Spearman*		*Kendall*	
	Rho	*P-Value*	*Tau B*	*P-Value*
RISK_LEVEL – AGE	-0.14	0.142	-0.121	0.142
RISK_LEVEL – GENDER	-0.159	0.098	-0.149	0.097
RISK_LEVEL – EDUCATION	-0.216	0.023	-0.195	0.025
RISK_LEVEL – G1	0.433	<0.001	0.396	<0.001
RISK_LEVEL – G2	0.719	<0.001	0.6	<0.001
RISK_LEVEL – G3	0.421	<0.001	0.389	<0.001
RISK_LEVEL – G4	0.74	<0.001	0.62	<0.001
G1 – G2	0.281	0.003	0.225	0.004
G1 – G3	0.04	0.678	0.037	0.678
G1 – G4	0.435	<0.001	0.35	<0.001

Additionally, the presence of cybersecurity teams positively influences computer security awareness and adherence to security policies and data handling practices among employees. However, there is no significant correlation between G1 and G3 (password and account security), as indicated by the *P*-values ($P > 0.05$).

Demographic Information

The dataset comprised responses from participants across various age groups, with the age categories defined as follows: 18–24 years (Code: 1), 25–34 years (Code: 2), 35–44 years (Code: 3), 45–54 years (Code: 4), and above 54 years (Code: 5). The data shows that the most frequent age group among the respondents was 18–24-year age group (35.5%), followed by the 25–34-year group (30.9%) and the 35–44-year age group (14.5%). There was a small representation of respondents in the 45-–54 years old (8.2%), and those in the 55-years-and-above group made up 10.9% of the respondents.

The distribution shows that most respondents fell within the younger and middle-aged segments, namely 18–34 years, while the older age groups had a relatively minor representation in the dataset. The calculated SD is approximately 1.321, and the variance is approximately 1.745, indicating that the respondents' ages were not widely spread and were concentrated around specific age groups. As shown in Figure 3, the demographic information by age reveals essential trends in our population's age distribution.

Moreover, the data shows that the gender distribution of the respondents was relatively evenly split, with 34.5% of respondents being female, 63.6% being male, and 1.8% indicating "other." This distribution provides valuable insights into the sample composition, shedding light on gender representation among participants. The calculated SD of 0.508 contributes an additional layer of understanding, indicating the extent of variability in the gender distribution data. This value signifies a moderate dispersion of responses around the mean gender percentages. Figure 4 presents demographic information by gender, offering valuable insights into the composition of our population.

Furthermore, the variance of 0.258 complements the SD by quantifying the spread of data points within the gender distribution. The relatively low variance value suggests that the distribution is fairly consistent, with responses clustered around the mean proportions of female and male participants.

In analyzing the participants' education levels, a transparent distribution emerged between the various academic degrees, and additional statistical measures enhanced our understanding of the data's dispersion. Most respondents, comprising 69.1% of the sample, held bachelor's degrees, showing a significant representation of individuals with undergraduate education in the surveyed population.

Figure 3. Demographic information by age

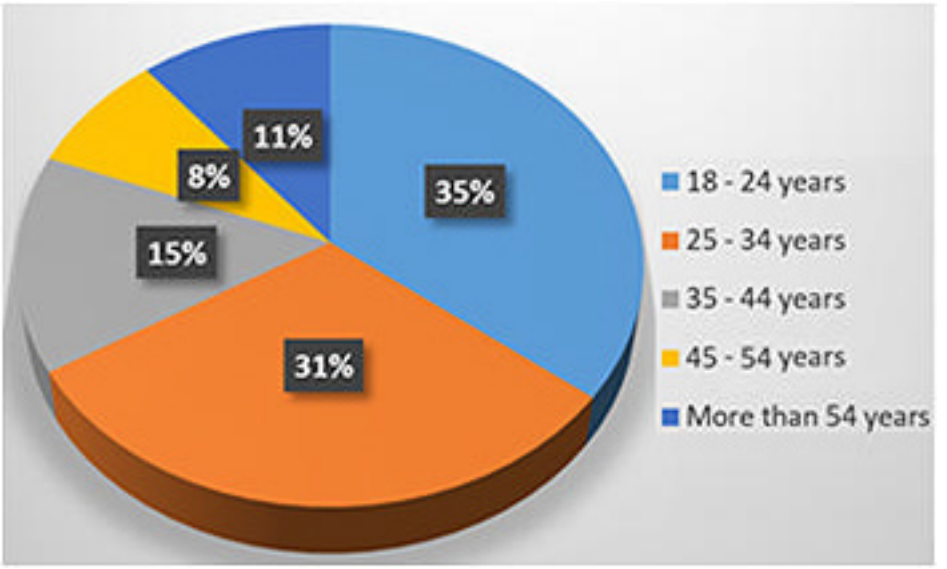
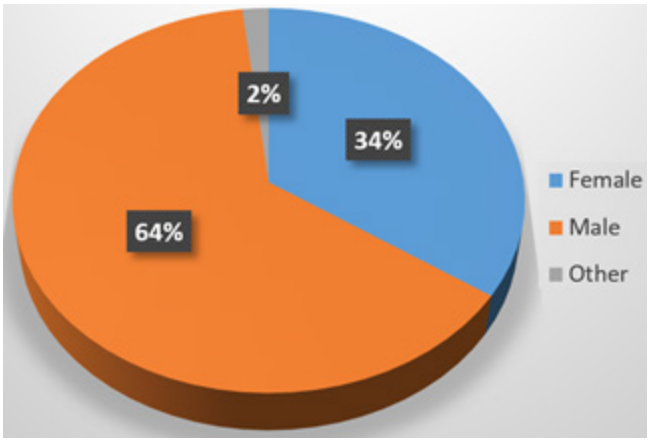


Figure 4. Demographic information by gender



Additionally, 18.2% of participants reported having master's degrees, indicating a notable proportion of individuals pursuing further postgraduate studies. However, 12.7% of participants had completed only high school education. In Figure 5, the demographic information by education level highlights the educational attainment levels of our population.

The calculated SD of 0.555 adds an essential dimension to our analysis by quantifying the extent of variability within the data. This measure indicates that the responses regarding education levels exhibit relatively low dispersion around the mean. In other words, the distribution of participants across degrees is fairly concentrated, with limited deviations from the overall proportions.

The variance of 0.308 aligns with the SD, providing further insight into the spread of data points around the mean. The relatively low variance indicates that the education levels are clustered around the mean percentages of each degree holder, suggesting a consistent distribution without extreme variations.

Figure 5. Demographic information by education level

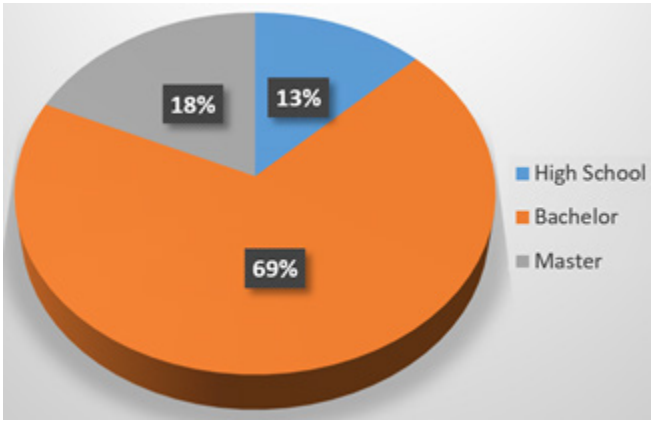
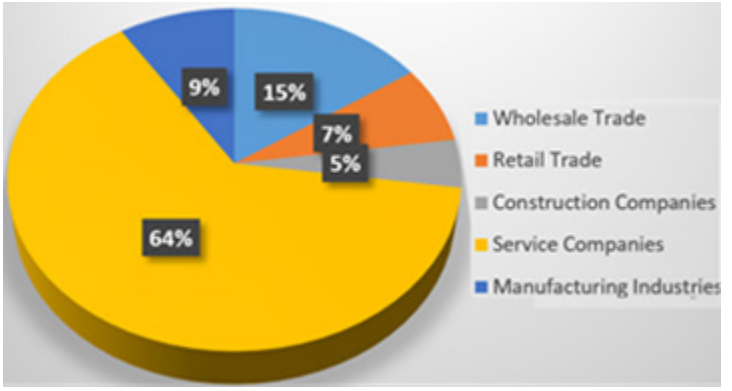


Figure 6. Demographic information by industry distribution



Regarding industry distribution, the percentages reveal the representation of different sectors within the dataset. Notably, "Service Companies" had more representation, with 63.6%, indicating a significant presence in the dataset. "Wholesale Trade" held a share of 15.5%, while "Retail Trade" and "Manufacturing Industries" represented 7.3% and 9.1%, respectively. "Construction Companies" made up 4.5% of representation. The SD 1.230 indicates moderate data variability, while the variance 1.514 aligns with it. Thus the data is representative of the distribution of different sectors. Figure 6 focuses on demographic information by industry, presenting the distribution of individuals across various sectors and giving valuable insights into our workforce composition.

DISCUSSION

Table 6 presents an overview of the results obtained from testing various hypotheses related to cybersecurity risk factors among employees. The hypotheses include diverse factors, including age, gender, education, security practices, and the influence of cybersecurity teams, all contributing to our understanding of employees' cybersecurity risk levels.

Table 6. Results of hypotheses testing

Hypothesis	*Result*
H1: There is a significant correlation between the level of cyber risk and the age of employees.	*Not supported*
H2: There is a significant correlation between the level of cyber risk and employees' gender	*Not supported*
H3: There is a significant correlation between the level of cyber risk and the educational level of employees	*Supported*
H4: The presence of cybersecurity teams is positively correlated with employees' cyber risk level	*Supported*
H5: Strong password management and account security practices are associated with lower employee risk levels	*Not supported*
H6: Adherence to security policies and responsible data handling are associated with lower employee risk levels	*Supported*
H7: Cybersecurity knowledge and general awareness are associated with lower employee risk levels	*Supported*
H8: The presence of security teams in the organization positively influences employees' awareness of computer security and response capacity	*Supported*
H9: The presence of security teams in the organization positively influences employees' proper management of passwords and account security	*Not supported*
H10: The presence of security teams in the organization positively influences the adoption of security policies and the responsible management of data among employees	*Supported*

Determinants of Employee's Risk Levels

The results of this study reveal that age does not significantly influence an employee's cybersecurity risk level. This finding challenges the prevailing stereotype that associates older employees with lower levels of technological competence and greater susceptibility to cybersecurity threats. Instead, it underscores the need for inclusive cybersecurity training programs that cater to employees of all ages. Similarly, our study highlights that cybersecurity awareness and risk levels are unrelated to gender-specific factors.

Accordingly, cybersecurity teams are encouraged to be mindful of providing cybersecurity awareness training and initiatives that promote equity and inclusion, regardless of gender considerations. Furthermore, the results reveal an interesting trend: employees with higher levels of education tend to demonstrate greater awareness of cybersecurity best practices and show a better ability to identify potential threats.

Social capital is crucial to improving collaboration and information sharing within organizations, especially cybersecurity initiatives. Strong internal networks foster open communication, allowing employees to collaborate effectively and share knowledge. By leveraging these networks, cybersecurity teams improve overall security awareness and policy compliance, although their influence on practices such as password management may require more targeted interventions. Ultimately, social capital strengthens an organization's ability to anticipate and respond to cyber threats, contributing to a more resilient security posture.

Improving Cybersecurity Risk Levels

An effective cybersecurity team mitigates employees' overall risk levels within an organizational context. Our results suggest that a cybersecurity team generates a higher sense of security among employees. Consequently, compliance with security policies and a higher awareness of cybersecurity show strong correlations with a lower level of risk, allowing employees to better deal with a threat for which they are prepared than employees unaware of existing threats on the Internet or in other digital contexts.

Cultural intelligence plays a critical role in this dynamic, as cybersecurity teams equipped with high cultural intelligence can adapt their training to address diverse cultural perspectives and learning styles within the organization. This adaptability fosters effective communication and engagement, improving cybersecurity awareness and practices. As a result, employees are better prepared to deal with complex cyber threats, ultimately reducing overall risk levels.

The impact of Security Teams

The incorporation of a cybersecurity team into organizational structures positively influences various aspects of cybersecurity practices among employees. Our findings suggest that organizations equipped with dedicated cybersecurity teams contribute to promoting a high-cybersecurity culture.

Cybersecurity teams should actively facilitate organizational security instead of reactive measures against cybersecurity threats. Moreover, the most relevant impact of the cybersecurity team at any organization is not the integration of a cybersecurity framework or the adoption of different technologies, but the promotion of cybersecurity awareness among employees through courses, talks, hands-on activities, and simulations that present the real impact of a cyber attack and show how this kind of incident can affect their jobs.

CONCLUSIONS AND FUTURE RESEARCH

This study contributes to a multifaceted picture of cybersecurity culture among employees in organizational settings. The findings show that age is not a significant factor, refuting the misconception that older employees are inherently less tech-savvy and more susceptible to cybersecurity threats. Accordingly, the study underscores the importance of inclusive cybersecurity training programs targeting people of all age groups.

Similarly, gender was found to have no bearing on employees' cybersecurity risk levels, emphasizing that cybersecurity awareness and risk perception transcend gender-specific factors. Consequently, organizations should adopt gender-neutral approaches in their cybersecurity training and awareness initiatives.

Furthermore, the study highlights the positive influence of higher education levels on employees' cybersecurity awareness, ability to identify threats, and adherence to security policies. Accordingly, organizations are encouraged to tailor their cybersecurity training programs to accommodate diverse educational backgrounds, ensuring comprehensive coverage and risk mitigation.

Integrating cybersecurity teams within organizational structures has substantially impacted cybersecurity practices and employee awareness. Cybersecurity teams are instrumental in increasing employee awareness of an organization's cybersecurity. Additionally, cultural intelligence plays a critical role by fostering employees' ability to navigate diverse cybersecurity challenges and adapt to varying contexts. Cultural intelligence enhances training programs' effectiveness by promoting understanding and engagement across different cultural and organizational environments.

Moreover, social capital is a critical factor that strengthens employee collaboration and information sharing. Organizations can enhance their collective intelligence and resilience against cybersecurity threats by cultivating solid internal networks and relationships. Cybersecurity teams that leverage this social capital are better equipped to drive policy adherence, foster a culture of security, and elevate overall risk awareness.

Our study has some limitations. First, the relatively small sample size of 110 surveys and the use of self-reported data may impact the generalizability and accuracy of the findings. Second, the study's focus on León City limits its applicability to the diversity within the population of Mexico. Additionally, the cross-sectional design restricts insights into how cybersecurity risk levels change over time. Lastly, survey questions and design may introduce measurement errors.

Future research may address the limitations of this study by expanding the sample size to include a more diverse population from various states in Mexico or Latin America. Another avenue of research may use a longitudinal design.

CONFLICTS OF INTEREST

We wish to confirm that there are no known conflicts of interest associated with this publication.

FUNDING STATEMENT

No funding was received for this work.

INFORMED CONSENT STATEMENT

Informed consent for participation was obtained from all subjects involved in the study.

PROCESS DATES

Received: July 12, 2024, Revision: September 27, 2024, Accepted: October 5, 2024

CORRESPONDING AUTHOR

Correspondence should be addressed to Luis Mena; lmena@upsin.edu.mx

REFERENCES

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology*, *71*(8), 939–953. DOI: 10.1002/asi.24311

Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. *Computers & Security*, *98*(2), 102003. DOI: 10.1016/j.cose.2020.102003

Amankwa, E., Loock, M., & Kritzinger, E. (2021). Information security policy compliance culture: Examining the effects of accountability measures. *International Journal of Technology and Human Interaction*, *17*(4), 75–91. DOI: 10.4018/IJTHI.2021100105

Berlilana, N., Noparumpa, T., Ruangkanjanases, A., Hariguna, T., & Sarmini, . (2021). Organization benefit as an outcome of organizational security adoption: The role of cyber security readiness and technology readiness. *Sustainability (Basel)*, *13*(24), 13761. DOI: 10.3390/su132413761

Bond, T. (2012). *Employee security awareness survey*. Scribd. https://es.scribd.com/document/493941870/employee-security-awareness-survey

Burrell, D. N., Springs, D., Burton, S. L., Dawson, M., Wright, J. B., & Modeste, R. (2020). Perspectives in talent management strategies for cybersecurity job roles in public safety and health in government organizations. *International Journal of Smart Education and Urban Society*, *11*(4), 1–17. DOI: 10.4018/IJSEUS.2020100101

Cabral, Â. M. R., Carvalho, F. M. P. O., & Ferreira, J. A. V. (2020). The effect of emotional and cultural intelligences on networks' behaviors in international SMEs: Evidence from Portugal. *Behavioral Sciences (Basel, Switzerland)*, *10*(11), 163. DOI: 10.3390/bs10110163 PMID: 33114445

Chaudhary, S. (2024). Driving behaviour change with cybersecurity awareness. *Computers & Security*, *142*(C), 103858. DOI: 10.1016/j.cose.2024.103858

Crowne, K. A. (2008). What leads to cultural intelligence? *Business Horizons*, *51*(5), 391–399. DOI: 10.1016/j.bushor.2008.03.010

Dalal, R. S., Howard, D. J., Bennett, R. J., Posey, C., Zaccaro, S. J., & Brummel, B. J. (2022). Organizational science and cybersecurity: Abundant opportunities for research at the interface. *Journal of Business and Psychology*, *37*(1), 1–29. DOI: 10.1007/s10869-021-09732-9 PMID: 33564206

Erendor, M. E., & Yildirim, M. (2022). Cybersecurity awareness in online education: A case study analysis. *IEEE Access: Practical Innovations, Open Solutions*, *10*(4), 52319–52335. DOI: 10.1109/ACCESS.2022.3171829

Evans, M., Maglaras, L. A., He, Y., & Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks*, *9*(17), 4667–4679. DOI: 10.1002/sec.1657

Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, *59*(2), 26–44. DOI: 10.1016/j.cose.2016.01.004

Georgiadou, A., Michalitsi-Psarrou, A., & Askounis, D. (2021a). Evaluating the cyber-security culture of the EPES sector: Applying a cyber-security culture framework to assess the EPES sector's resilience and readiness. In *ARES '22: Proceedings of the 17th International Conference on Availability, Reliability and Security* (pp. 1-10). Association for Computing Machinery. DOI: 10.1145/3538969.3543813

Georgiadou, A., Michalitsi-Psarrou, A., & Askounis, D. (2023, June). A security awareness and competency evaluation in the energy sector. *Computers & Security*, *129*, 103199. DOI: 10.1016/j.cose.2023.103199

Georgiadou, A., Michalitsi-Psarrou, A., Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Doukas, G., Ntanos, C., Landeiro-Ribeiro, L., & Askounis, D. (2021b). Hospitals' cybersecurity culture during the COVID-19 crisis. *Health Care*, *9*(10), 1335. DOI: 10.3390/healthcare9101335 PMID: 34683015

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022a). Working from home during COVID-19 crisis: A cyber security culture assessment survey. *Security Journal*, *35*(2), 486–505. https://link.springer.com/article/10.1057/s41284-021-00286-2. DOI: 10.1057/s41284-021-00286-2

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022b). A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems*, *62*(3), 452–462. DOI: 10.1080/08874417.2020.1845583

Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Georgiadou, A., Michalitsi-Psarrou, A., Doukas, G., Kontoulis, M., Nikoloudakis, Y., Marin, S., Cabecinha, R., & Ntanos, C. (2022). A cybersecurity culture survey targeting healthcare critical infrastructures. *Health Care*, *10*(2), 327. DOI: 10.3390/healthcare10020327 PMID: 35206941

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. *Journal of Information Security and Applications*, *58*(4), 102726. DOI: 10.1016/j.jisa.2020.102726

Kam, H. J., Menard, P., Ormond, D., & Crossler, R. E. (2020, May). Cultivating cybersecurity learning: An integration of self-determination and flow. *Computers & Security*, *96*, 101875. DOI: 10.1016/j.cose.2020.101875

Khan, N. F., Yaqoob, A., Khan, M. S., & Ikram, N. (2022). The cybersecurity behavioral research: A tertiary study. *Computers & Security*, *120*(10), 102826. DOI: 10.1016/j.cose.2022.102826

Klimburg-Witjes, N., & Wentland, A. (2021). Hacking humans? Social engineering and the construction of the "deficient user" in cybersecurity discourses. *Science, Technology & Human Values*, *46*(6), 1316–1339. DOI: 10.1177/0162243921992844

Kweon, E., Lee, H., Chai, S., & Yoo, K. (2021). The utility of information security training and education on cybersecurity incidents: An empirical evidence. *Information Systems Frontiers*, *23*(2), 361–373. DOI: 10.1007/s10796-019-09977-z

Li, M., Mobley, W. H., & Kelly, A. (2016). Linking personality to cultural intelligence: An interactive effect of openness and agreeableness. *Personality and Individual Differences*, *89*, 105–110. DOI: 10.1016/j.paid.2015.09.050

Martins, C., & Medeiros, I. (2022). Generating quality threat intelligence leveraging OSINT and a cyber threat unified taxonomy. *ACM Transactions on Privacy and Security*, *25*(3), 1–39. DOI: 10.1145/3530977

Ogbanufe, O. (2021). Enhancing end-user roles in information security: Exploring the setting, situation, and identity. *Computers & Security*, *108*(0167), 102340. DOI: 10.1016/j.cose.2021.102340

Onumo, A., Ullah-Awan, I., & Cullen, A. (2021). Assessing the moderating effect of security technologies on employees compliance with cybersecurity control procedures. *ACM Transactions on Management Information Systems*, *12*(2), 1–29. DOI: 10.1145/3424282

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition Technology and Work*, *24*(2), 371–390. DOI: 10.1007/s10111-021-00683-y PMID: 34149309

Ponemon Institute & IBM Security. (2019). *Cost of a data breach report*. https://www.ibm.com/downloads/cas/RDEQK07R

Pratama, A. R., Firmansyah, F. M., & Rahma, F. (2022). Security awareness of single sign-on account in the academic community: The roles of demographics, privacy concerns, and Big-Five personality. *PeerJ. Computer Science*, *8*(2), e918. DOI: 10.7717/peerj-cs.918 PMID: 35494842

Puth, M. T., Neuhäuser, M., & Ruxton, G. D. (2015). Effective use of Spearman's and Kendall's correlation coefficients for association between two measured traits. *Animal Behaviour*, *102*, 77–84. DOI: 10.1016/j.anbehav.2015.01.010

Rahim, N. H., Hamid, S., Kiah, M. L. M., Shamshirband, S., & Furnell, S. (2015). A systematic review of approaches to assessing cybersecurity awareness. *Kybernetes*, *44*(4), 606–622. DOI: 10.1108/K-12-2014-0283

Renaud, K., Von Solms, B., & Von Solms, R. (2019). How does intellectual capital align with cyber security? *Journal of Intellectual Capital*, *20*(5), 621–641. DOI: 10.1108/JIC-04-2019-0079

Rodgers, W., Alhendi, E., & Xie, F. (2019). The impact of foreignness on the compliance with cybersecurity controls. *Journal of World Business*, *54*(6), 101012. DOI: 10.1016/j.jwb.2019.101012

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65–78. DOI: 10.1016/j.cose.2015.05.012

Safi, R., & Browne, G. J. (2023). Detecting cybersecurity threats: The role of the recency and risk compensating effects. *Information Systems Frontiers*, *25*(3), 1277–1292. DOI: 10.1007/s10796-022-10274-5

Schühly, A. M. (2022). *Cultural influences on the process of strategic management: Using scenario planning for decision making in multinational corporations* Springer. https://link.springer.com/book/10.1007/978-3-030-86660-0

Security, I. B. M. (2022). *X-Force threat intelligence index 2022*. https://www.ibm.com/downloads/cas/ADLMYLAZ

Seibert, S. E., Kraimer, M. L., & Liden, R. C. (2001). A social capital theory of career success. *Academy of Management Journal*, *44*(2), 219–237. https://www.researchgate.net/publication/228831713_A_Social_Capital_Theory_of_Career_Success. DOI: 10.2307/3069452

Thangavelu, M., Krishnaswamy, V., & Sharma, M. (2021). Impact of comprehensive information security awareness and cognitive characteristics on security incident management—An empirical study. *Computers & Security*, *109*(5), 102401. DOI: 10.1016/j.cose.2021.102401

Tjirare, D., & Shava, F. B. (2020). Developing security metrics to evaluate employee awareness: A case of a ministry in Namibia. *Namibian Journal for Research. Science and Technology*, *1*(1), 11–18. DOI: 10.54421/njrst.v1i1.5

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *Computers & Security*, *52*, 128–141. DOI: 10.1016/j.cose.2015.04.006

APPENDIX

Table 7. Survey instrument: Employee security awareness survey

#	*Question*	*Group*
1	*What is your position within the company?*	*Does not apply*
2	*Do you have a cybersecurity team?*	*G* 1
3	*Do you know who to contact in case you are hacked or if your computer is infected?*	*G* 2
4	*Have you ever found a virus or Trojan on your computer at work?*	*G* 2
5	*Do you know how to tell if your computer is hacked or infected?*	*G* 2
8	*How secure do you feel your computer is?*	*G* 2
9	*Is the firewall on your computer enabled?*	*G* 2
10	*Is your computer configured to be automatically updated?*	*G* 2
11	*How careful are you when you open an attachment in email?*	*G* 2
12	*Do you know what a phishing attack is?*	*G* 2
13	*Do you know what an email scam is and how to identify one?*	*G* 2
14	*Is anti-virus currently installed, updated, and enabled on your computer?*	*G* 2
15	*My computer has no value to hackers; they do not target me.*	*G* 2
20	*Have you downloaded and installed software on your computer at work?*	*G* 2
6	*Have you ever given your password from work to someone else?*	*G* 3
21	*Has your boss or anyone else you know at work asked you for your password?*	*G* 3
22	*Do you use the same passwords for your work accounts as you do for your personal accounts at home, such as Facebook, Twitter, or your personal email accounts?*	*G* 3
7	*If you format a hard drive or erase the files on it, all the information on it is permanently lost.*	*G* 4
16	*Does your company have policies on which websites you can visit?*	*G* 4
17	*Does your company have policies on how what you can and cannot use email for?*	*G* 4
18	*Is instant messaging allowed in your organization?*	*G* 4
19	*Can you use your own personal devices, such as your mobile phone, to store or transfer confidential company information?*	*G* 4
23	*How often do you take information from the office and use your computer at home to work on it?*	*G* 4
24	*Have you logged into work accounts using public computers, such as from a library, cybercafe, or hotel lobby?*	*G* 4

Rafael Martínez-Peláez received a doctorate degree from the Technical University of Catalonia (Spain) in 2010. He is professor in the department of systems engineering and computing of the Northern Catholic University in Chile and the Polytechnic University of Sinaloa. He has served as TPC member of many international conferences and workshops. He is a level I researcher of the National System of Researchers of Mexico. His research interests include cybersecurity, digital transformation, and electronic services.

Dr. Velarde holds a Bachelor of Science degree in electronics engineering from the Autonomous University of Guadalajara in 1993. The Master´s and Doctor's in Sciences degree in Electrical Engineering from the Center for Research and Advanced Studies of the National Polytechnic Institute in 2001 and 2009, respectively. Currently, he is a research professor at the academic unit of basic sciences and engineering of the Autonomous University of Nayarit. . He is a level I researcher of the National System of Researchers of Mexico. He is in charge of the Computer Security and Artificial Intelligence Research Laboratory (https://securitylab.uan.mx/). He has been author and co-author of journal papers and conference proceedings, director and co-director of undergraduate and graduate theses in different institutions. He is also technical manager of funded research projects. His research lines of interest are directed to the use of artificial intelligence in problems related to security in data networks and oral health (cephalometric studies and caries detection).

Vanessa G. Félix is a Doctor of Education with a Master's degree in administrative information systems and a Bachelor's degree in computer science. She currently works as a researcher and full-time professor in the academic programs of engineering in information technology and master of applied sciences at the Polytechnic University of Sinaloa, and assistant professor of the Autonomous University of the West. Her teaching activities are mainly developed in the topics systems analysis, systems design and software engineering. Her main research activities are carried out within the Consolidated Academic Group of Information Technology and Applied Communications in the lines of educational technology and technologies applied to the health sector. She is level I researcher of the National System of Researchers of Mexico in the physics-mathematics area and honorary member of the System of Researchers and Technologist of Sinaloa. She has published more than 40 refereed articles in indexed journals and conference proceedings of recognized prestige. Her main research interests include the use of emerging computing technologies to address problems in the health, education, and productive sectors, especially through the development of software systems based on mobile computing.

Alberto Ochoa received the electronic and telecommunication engineering degree from University of Colima (Mexico) in 1999; and the doctorate degree in electronics from the University of Alcala (Spain) in 2007. Since 2008, he has been a lecturer and researcher at the electronics department of the University of Colima in Mexico. In this period he has collaborated in several educational and research projects in the area of electronic and sensorial systems for mobile robots, ultrasonic signal processing applied in robotics, embedded systems and computing architectures for local positioning systems, and more recently in the development of intelligent algorithms applied to biomedical signals for segmentation of ECG signals and pattern recognition for medical diagnosis and prognosis, as well as the development of mobile computing systems for personal health monitoring. He is a level I researcher of the National System of Researchers of Mexico. In addition, he has published more than 40 peer-reviewed articles in prestigious journals and conference proceedings.

Rodolfo Ostos is a Master of Science from the University of the West, Mazatlan Unit (2006) and a Doctor in electrical engineering from the Center for Research and Advanced Studies of the National Polytechnic, Unit Guadalajara (2015) in the area of computing. He is a full-time research professor and director of the information technology engineering career at the Polytechnic University of Sinaloa, and assistant professor of the Autonomous University of the West. He is a member of the System of Researchers and Technologist of Sinaloa and a level I researcher of the National System of Investigators of Mexico. His main research interests are oriented to the development of multi-agent systems, distributed systems and medical monitoring systems.

Luis J. Mena obtained a doctorate in computer science in 2008 at the National Institute of Astrophysics, Optics and Electronics (Mexico), he also has a Master's degree in applied computing and a Bachelor's degree in computing at the University of Zulia (Venezuela). He currently works as a full-time professor at the Polytechnic University of Sinaloa, and leader of the Consolidated Academic Group of Information Technology and Applied Communications. He is a level II national researcher of Mexico in the interdisciplinary area and honorary researcher of the System of Researchers and Technologist of Sinaloa. Among his main scientific findings are: the development of an algorithm to measure the variability of blood pressure, which has allowed opening new fields of research regarding the clinical value of this phenomenon, and a symbolic binary classification algorithm to extract patterns from unbalanced clinical data sets. In addition, he has published more than 90 peer-reviewed articles in prestigious journals and conference proceedings. His main research interests include pattern recognition for medical diagnosis and prognosis, as well as the development of mobile computing systems for personal health monitoring.