Examining cybersecurity culture in Leon city organizations: Insights from 2022

Examinando la cultura de ciberseguridad en las organizaciones de la ciudad de León: percepción de 2022

Francisco Javier García Arellano[1] https://orcid.org/0009-0003-5061-7746
Ítalo Donoso Barraza[2] https://orcid.org/0009-0006-0468-9919
Angélica Flores Bustos[2] https://orcid.org/0009-0007-8989-6809
Carlos Pon Soto[2] https://orcid.org/0009-0003-1657-5626
Víctor Flores Fonseca[2] https://orcid.org/0000-0002-6995-9434
Rafael Martínez-Peláez[2*] https://orcid.org/0000-0003-2188-9892

Recibido 5 de abril de 2024, aceptado 28 de mayo de 2024
Received: April 05, 2024 Accepted: May 28, 2024

ABSTRACT

Recent research indicates that public and private organizations worldwide face cybersecurity breaches due to a need for more cybersecurity awareness among their employees. This study assesses the cybersecurity culture in different organizations across various sectors in Leon City, Mexico. For this purpose, an evaluation process was implemented, which involved anonymous online surveys among employees from multiple sectors, including service companies, wholesale trade businesses, manufacturing industries, construction companies, and retail trade establishments. The study took place in 2022 and achieved a response rate of 73.33% from employees across the participating organizations. The findings underscore the necessity of fostering a robust cybersecurity culture within Leon City organizations, which entails implementing ongoing security awareness training programs to empower employees with the knowledge and skills to mitigate cyber risks effectively. Analyzing the results reveals valuable insights regarding the countermeasures implemented by organizations in Leon City to strengthen their cybersecurity defenses and minimize the risk surface. These insights enhance cybersecurity strategies and fortify the overall security posture of organizations operating in Leon City.

Keywords: Awareness, cyber-attacks, cybersecurity, information security, risk.

RESUMEN

Investigaciones recientes indican que organizaciones públicas y privadas en todo el mundo enfrentan brechas de ciberseguridad debido a la falta de conciencia de ciberseguridad entre sus empleados. Este estudio evalúa la cultura de ciberseguridad en diversas organizaciones de varios sectores en la ciudad de León, México. Con este propósito, se implementó un proceso de evaluación que incluyó encuestas en línea anónimas entre empleados de múltiples sectores, como empresas de servicios, negocios mayoristas, industrias manufactureras, empresas de construcción y establecimientos de comercio minorista. El estudio se llevó a cabo en 2022 y logró una tasa de respuesta del 73,33% de empleados de las organizaciones

[1] Universidad La Salle Bajío, Facultad de Ingenierías y Tecnologías. León, México. Email: ing.f_javier@outlook.com
[2] Universidad Católica del Norte, Departamento de Ingeniería de Sistemas y Computación. Antofagasta, Chile. Email: italo.donoso@ucn.cl; angelica.flores@ucn.cl; cpon@ucn.cl; vflores@ucn.cl; rafael.martinez@ucn.cl
* Autor de correspondencia: rafael.martinez@ucn.cl

participantes. Los hallazgos subrayan la necesidad de fomentar una sólida cultura de ciberseguridad dentro de las organizaciones en la ciudad de León, lo cual implica implementar programas continuos de capacitación en conciencia de seguridad para dotar a los empleados de los conocimientos y habilidades necesarios para mitigar de manera efectiva los riesgos cibernéticos. Al analizar los resultados, surgen percepciones valiosas sobre las contramedidas implementadas por las organizaciones en León para fortalecer sus defensas de ciberseguridad y minimizar la superficie de riesgo. Estas percepciones mejoran las estrategias de ciberseguridad y fortalecen la postura de seguridad general de las organizaciones que operan en la ciudad de León.

Palabras clave: Concientización, ciberataques, ciberseguridad, seguridad de la información, riesgo.

INTRODUCTION

Cybersecurity has become one of the dominant domains in both public and private organizations [1]-[3]. Over the past decades, various scientific efforts have been made to identify, classify, and address vulnerabilities and weaknesses in these organizations [1]-[5]; however, more than these efforts are needed to deter the continuously evolving cybercrime. Under this circumstance, the coronavirus outbreak has further exacerbated the increase in cybercrime [4]. Critical infrastructures, including energy and healthcare sectors, have become prime targets [2], [5]-[7]. In particular, hospitals have experienced patient data loss, ransomware attacks, and availability threats.

While security infrastructure plays a critical role in defending against cybercriminal tactics and techniques, organizations recognize that their personnel pose the biggest threat to privacy and security [8]. Research indicates that over 39% of security risks can be attributed to human factors, and an overwhelming 95% of successful cyber-attacks stem from human error, with a significant portion originating from insider threats [9].

In recent years, significant scientific efforts have been made to assess the cybersecurity readiness of employees in public and private organizations [10]. A holistic approach has been adopted, and "cybersecurity culture" has emerged. Cybersecurity culture encompasses the attitudes, behavior, knowledge, and awareness organizational personnel display regarding common cyber risks and threats to protect information assets [11]-[13]. Assessing cybersecurity culture involves focused campaigns, education programs, ICT infrastructure audits, and the reassessment of security policies to cultivate a culture of responsibility and prevent attacks or data breaches [14]. Surveys conducted in various countries have highlighted the need for more employee cybersecurity training [5], [7], [15], [16]. At the same time, other studies have emphasized the role of human error, lack of security culture, awareness, and employee negligence in security incidents [17].

This study analyses the overall disposition towards cybersecurity in private organizations, focusing on the impact of cybersecurity awareness among employees on cybersecurity practices. The assessment includes organizations from different sectors, focusing on understanding the cybersecurity culture within these organizations.

BACKGROUND

Cybersecurity risks and threats against SMEs

Amid a global crisis, cybercriminals have stepped up their attacks against unsuspecting businesses and individuals, exploiting vulnerabilities introduced by digital adoption. In small and medium-sized businesses (SMEs), common cyberattacks and threats that transcend the organization's internal security limits have emerged [18]-[20]. Cybercriminals employ a strategic approach by developing deceptive browsing applications and adapting their schemes to exploit the weaknesses of end users. Upon installation, these applications automatically launch browsers and discreetly capture the victim's credentials.

At the same time, malicious users take advantage of users' lack of knowledge to compromise the confidentiality, integrity, and availability of data. Malicious users can assume the appearance of legitimate employees to conduct financial transactions, resulting in monetary losses and

unauthorized access to sensitive organizational information. The spectrum of cyber threats is expanding as hackers diversify their tactics, incorporating denial of service (DoS) attacks targeting public and private organizations or exploiting fake or malicious social media accounts to spread false information, and deceive users into revealing their login credentials. The proliferation of phishing websites on social media further amplifies the risk of credential theft.

Hackers expand their reach into web-based deception by creating websites imputing reputable organizations. These unauthorized sites serve as conduits to trick users and collect sensitive information. The persistent threat of malware, including viruses, spyware, and Trojans, poses a significant risk to personal devices and corporate systems. Cybercriminals leverage various vectors to spread malware, including crisis-related interactive maps, websites, and spam emails.

Additionally, mobile users face different threat situations. Fraudulent apps, themed around the crisis, are emerging, capable of locking users' devices and demanding a ransom or surreptitiously harvesting credentials. Additionally, access to unsecured public Wi-Fi networks exposes users to potential attacks. A worrying trend that transcends crises involves ransomware targeting critical institutions, including hospitals, educational entities, and public organizations. This malicious software locks users out of their systems, and cybercriminals demand a ransom for system release. Rogue applications and compromised credentials are common infection vectors. The broad scope of cyber threats extends to spam emails, regardless of the prevailing crisis. Scammers and hackers send phishing emails with crisis-related messages, tricking victims into divulging personal information or contributing cryptocurrency.

Predictions from the World Bank, the World Health Organization, the World Economic Forum, and the Centers for Disease Control and Prevention underscore the potential global financial losses resulting from these cyber-attacks and threats. This highlights the urgent need for investment in cybersecurity, reflecting the insights of esteemed institutions contributing to the discourse on the economic impact of these malevolent cyber activities [21].

Consequences of cyberattacks on SMEs

After a cyber-attack, SMEs around the world can face several significant consequences [22], [23]:

- Financial Impact: A cyberattack can result in financial losses for SMEs, including theft of corporate and financial information, theft of money, disruption to trading (e.g., inability to carry out online transactions), and loss of business or contracts. Additionally, companies may incur costs for repairing affected systems, networks, and devices.
- Increased Prices: The costs incurred from a cybercrime incident can lead businesses, including SMEs, to raise prices to cover expenses, which may result in some customers seeking more affordable alternatives, impacting sales and market competitiveness.
- Indirect Costs and Operational Disruption: In addition to direct financial losses, cyber-attacks can have indirect costs on business operations, including unexpected downtime, loss of productivity, and decreased employee morale. Small businesses heavily affected by an attack may need help to pursue business growth and handle their responsibilities. Operational disruption can also result in lost revenue.
- Legal Consequences: SMEs must manage the security of personal data they hold, whether it belongs to their staff or customers. Businesses may face fines and regulatory sanctions if this data is compromised due to a cyber-attack and appropriate security measures are not in place. Compliance with data protection and privacy laws is essential to avoid legal liabilities.
- Long-term Impact: A cyberattack can have long-lasting effects on a business's value and sustainability. It can damage a business's reputation, deter potential customers and investors, and affect employee recruitment.
- Reputational Damage: Trust is crucial for businesses, and a cyber-attack can damage the reputation of SMEs. It can erode customers' trust in them and lead to a loss of customers, sales, and profits. Reputational damage can also affect relationships with suppliers, partners, investors, and other third parties associated with the business.

To mitigate these consequences, SMEs must prioritize cybersecurity measures, including

implementing comprehensive cybersecurity plans, keeping software updated, training employees on cyberattack risks, using robust antivirus software, and having a well-defined incident response plan. Taking proactive steps to prevent cyber-attacks and promptly responding to incidents can help SMEs protect themselves and minimize potential damage.

Assessing human factors in cybersecurity

Assessing the cybersecurity capability of human agents, such as the workforce, is crucial for promoting practical workforce security consciousness. Several research studies have explored this area and proposed frameworks for assessing cybersecurity postures from the workforce perspective.

One such framework is the Human Factor Vulnerability Analysis (HFVA) presented by Kraemer and Carayon in [24]. The HFVA framework involves a three-stage process of identification, analysis, and solution to determine human-factor vulnerabilities associated with technical vulnerabilities. However, this framework relies on technical vulnerabilities. It assumes that human-factor vulnerabilities depend solely on them, which may only be partially true in the face of changing attack patterns [25].

Human agents' knowledge and experience of in cybersecurity play a significant role in their security perceptions and capabilities. Higher security proficiencies are typically associated with better decision-making capabilities influenced by experience. Domain knowledge in information and network security and practical knowledge acquired through hands-on practice are essential for effective intrusion detection and incident response [23].

Various assessment tools and techniques, such as interviews, questionnaires, observations, and gamification, have been used to evaluate security capabilities. Additionally, quantitative approaches have proven effective in evaluating the security capability of individuals and organizations, providing consistent results, and facilitating decision-making [8], [26].

The importance of human factors in information security must be considered. Human error and flawed decision-making contribute significantly to security breaches and cyber-attacks. Organizations must create a security-oriented culture where employees understand the importance of information security and are reluctant to circumvent security controls. Training, threat perception, and the organization's security culture influence end-user behavior and decision-making [16], [27].

Human performance and behavior in cybersecurity are complex issues that require the expertise of cognitive scientists and human factor experts. Understanding human behavior can help identify weaknesses, vulnerabilities, and critical phases of cybersecurity operations. Human factors initiatives should be integrated into the organizational culture to increase human performance and decision-making awareness [9], [25], [28].

The increasing number of cyber-attacks due to human error highlights the need to address human factors in cybersecurity: alert fatigue, operational fatigue, and cognitive overload, which challenge cybersecurity operators. Organizations must balance automated technologies and human factors, integrating strategic human factors objectives into their information strategies [10].

Cybersecurity awareness should encompass assessing human agents' cybersecurity capability, recognizing human factors' significance in information security, and integrating human factors initiatives into organizational culture [7]. By understanding and addressing human behavior, organizations can enhance their security posture and mitigate the risks of human error and decision-making.

Definition of cybersecurity culture

Cybersecurity culture refers to the collective attitudes, beliefs, values, and knowledge that individuals and organizations possess regarding cybersecurity practices and behaviors. It encompasses the intentional and unintentional ways cyberspace is utilized at different levels, including international, national, organizational, and individual perspectives [14].

At its core, cybersecurity culture promotes safety, security, privacy, and civil liberties in the digital realm. It involves understanding the risks and threats associated with cyberspace and adopting appropriate measures to protect information assets, critical infrastructure, and personal data [29].

Organizational culture serves as a foundation for cybersecurity culture. It defines how things are

done here within an organization and includes shared values, behaviors, and assumptions. An organizational culture that prioritizes information security and fosters responsible cyber behaviors is crucial in cybersecurity. This culture should be reflected in the values and basic assumptions within the organization [11].

From a broader perspective, cybersecurity culture extends beyond individual organizations to encompass a national and even international context. Cybersecurity culture becomes a collective responsibility with the internet's global connectivity and various technology devices. A national cybersecurity culture aims to maintain a cyber-environment that encourages efficiency, innovation, and economic prosperity while ensuring safety, security, business confidentiality, privacy, and civil liberties [30]. It involves protecting critical infrastructure, managing information assets, and minimizing cyber risks at the country level.

On an individual level, cybersecurity culture involves understanding the risks of utilizing cyberspace and taking necessary precautions to protect personal information, devices, and privacy. Users must exhibit behaviors contributing to the confidentiality, integrity, availability, and privacy of data and information assets for all parties involved, including being aware of potential threats, employing safe practices, and engaging in ethical and responsible online behavior.

While technology solutions play a significant role in cybersecurity, the human factor remains a crucial concern. Cyber users' attitudes, assumptions, beliefs, values, and knowledge greatly influence cybersecurity culture. Promoting a cybersecurity culture that encourages efficiency, innovation, and economic prosperity while upholding safety, security, privacy, quality, and civil liberties requires active participation and responsible behavior from individuals, organizations, and governments.

Measurement instruments such as surveys can be developed to assess and foster cybersecurity culture. These instruments should align with the theoretical perspectives and components of the cybersecurity culture model to ensure content validity. By understanding and measuring cybersecurity culture, stakeholders can identify areas for improvement, implement appropriate controls, and educate communities to cultivate a culture that prioritizes ethical, secure, and privacy-focused practices in cyberspace.

METHODOLOGY

This study aims to capture the perspective and the level of employee awareness among different economic sectors in Leon, Mexico. Figure 1 shows the methodology followed in this research [31].

a) Define Research Question: The first step in any research is formulating a straightforward, focused research question. This question should reflect the study's main objective and guide the entire research process. It serves as the foundation upon which the study is built and provides direction for data collection, analysis, and interpretation.
b) Selection of Survey: The survey selection marks the beginning of the research journey. This step carefully chooses a survey instrument to align with the research goals and objectives. The survey's validity and reliability are paramount, ensuring it measures the intended constructs effectively. The survey's content should be pertinent to the research context and the target population. A thorough review of available surveys and, if necessary, the creation of customized surveys ensure that the data collected adequately answers the research questions.
c) Data collected: Invitations are sent to potential participants once the survey is ready. These invitations serve as a crucial link between the research and the participants. The invitations should be clear and informative, explaining the purpose of the survey, its significance,

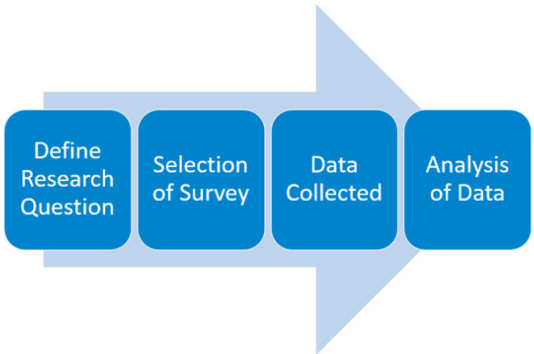

Figure 1. Methodology [31].

and the expected time commitment. Ethical considerations, including informed consent and data privacy, are emphasized. The invitations may be distributed via email, online platforms, or other appropriate channels. A user-friendly link to the survey and contact details for inquiries are provided to encourage participation and address any concerns.

d) Analysis of Data: After data collection, the analysis phase transforms raw data into meaningful insights. This step involves data cleaning, where inconsistencies or errors are identified and rectified. Descriptive statistics, such as averages, standard deviations, and frequencies, summarize the data's characteristics. The study answers research questions, validates hypotheses, and forms the basis for drawing conclusions and making informed recommendations.

Define research question

In the rapidly evolving context of cybersecurity, understanding the risk level among employees is a critical step toward fortifying organizations' digital defenses. León, Guanajuato, situated in the heart of Mexico, is an essential backdrop for this study, as it represents a dynamic hub of economic activities and technological advancements. This research initiative marks the first of its kind in the region, addressing the pivotal question:

RQ1: What is the risk level among employees in León, Guanajuato?

As the digital realm becomes increasingly integrated into various facets of daily operations, the vulnerabilities that come with it become more pronounced. The research question delves into uncharted territory, aiming to assess the risk employees face concerning cybersecurity awareness within the local context. By focusing on León, Guanajuato, this study intends to shed light on the challenges and opportunities this region presents, distinct from broader national or global assessments.

This research seeks to quantify the risk level and uncover the factors contributing to it. The study will explore the extent to which employees understand cybersecurity threats, are knowledgeable about preventive measures, and are aware of organizational policies. Through this multifaceted approach, the research aims to provide a comprehensive overview of cybersecurity awareness and preparedness among employees in León.

Furthermore, this study continues beyond identification; it looks ahead by probing into strategies for enhancing awareness and mitigation. With insights drawn from the risk assessment and a detailed examination of organizational practices, the research seeks to provide actionable recommendations to empower organizations in León to bolster their cybersecurity posture.

This study's geographical and contextual specificity offers invaluable insights for the local business community and the broader academic and professional spheres. This research addresses the pressing need for a localized understanding of cybersecurity risks and awareness, setting the foundation for future advancements in the field. As León advances its Mexico technology role, the results of this study have the potential to drive positive change, fostering a culture of cybersecurity awareness and ultimately safeguarding sensitive digital assets.

Selection of survey

The literature contains different surveys that evaluate the level of security awareness among individuals and organizations. These surveys serve as valuable tools for assessing cybersecurity knowledge, attitudes and practices, and provide insights into the overall security posture.

Researchers and practitioners have recognized the significance of security awareness in mitigating cyber risks and protecting sensitive information. Consequently, numerous studies have been conducted, introducing a range of surveys specifically designed to measure security awareness. For instance, Trenton Bond conducted the "Employee Security Awareness Survey" in 2012, which aimed to gauge the awareness level of employees in an organization [32]. This survey assessed employees' understanding of security concepts and adherence to security policies and practices.

Another notable survey is the "Cybersecurity Awareness Survey" conducted by the Centre for Cyber Safety and Education [33]. This survey seeks to evaluate the individuals' awareness regarding common cybersecurity threats, best practices, and

the potential consequences of security incidents. Additionally, studies have employed surveys such as "The impact of foreignness on the compliance with security controls," [34] "Assessing the moderating effect of security technologies on employees compliance with cybersecurity control procedures," [35] and "Cybersecurity culture survey targeting healthcare critical infrastructures" [5] to assess security awareness within specific contexts and sectors.

Other surveys address specific aspects of security awareness, such as the "Smartphone information security awareness" [36] and the "Cloud Security Awareness Survey" [37], which focus on understanding individuals' knowledge and behaviors related to mobile device security and cloud computing security, respectively.

Furthermore, surveys like the "Social Engineering Awareness Survey" delve into individuals' awareness of social engineering techniques and their ability to identify and respond to social engineering attacks.

Overall, these surveys play a crucial role in evaluating security awareness levels and identifying areas for improvement. By leveraging the insights gained from these assessments, organizations and researchers can develop targeted training programs, awareness campaigns, and security strategies to enhance individuals' and organizations' ability to defend against cyber threats. In particular, we decided to use the survey proposed by Trenton Bond because his survey offers the following benefits:

- Comprehensive assessment: The survey covers a wide range of security concepts, practices, and policies, providing a thorough evaluation of employees' security awareness. It explores various areas, including password management, data protection, social engineering and incident reporting.
- Standardized measurement: The survey employs standardized measurement scales and question formats, allowing for consistent and comparable results across respondents and organizations and facilitating benchmarking and analysis of security awareness levels over time.
- Informed decision-making: The survey results can provide valuable insights employees' security awareness' strengths and weaknesses. This information can guide decision-making processes, enabling organizations to prioritize and tailor their security training and awareness programs to address specific areas of improvement.
- Comparative analysis: As the survey has been widely used, its results can be compared with industry benchmarks and trends, enabling organizations to assess how they fare against similar organizations and identify areas where they may lag or excel in security awareness.
- Employee engagement: Conducting the survey demonstrates the organization's commitment to security and employee well-being. It can serve as an opportunity to engage employees in cybersecurity discussions and initiatives, fostering a culture of security awareness and responsibility.

Data collected

The data collection period lasted one month, from November 1st, 2022, to November 30th, 2022. Out of the 150 employees invited to participate, 110 participants visited the Google form and completed the online survey. The analysis in the following paragraphs includes the responses provided by the 110 participants who completed the survey.

RESULTS

Reliability

The results by item and the descriptive statistics of the data appear in Table 1. The reliability tests results demonstrate a satisfactory level of internal consistency for the survey instrument, with Cronbach $\alpha = 0.722$ and McDonald's $\omega = 0.732$. These values suggest that the survey items are reliably measure the intended constructs.

The descriptive statistics of the survey data, as presented in Table 1, provide valuable insights into the distribution and characteristics of each survey item. The mean (average) and standard deviation (SD) of each item give an overview of the central tendency and variability in participants' responses.

Items Q2, Q3, Q5, Q7, Q8, Q11, Q13, Q14, Q16, Q17, Q20, Q21, Q22, Q24, and Q25 all have means ranging between 1.1 and 3.327. These items pertain to various aspects of the survey and reflect participants' responses to different questions.

Table 1. Descriptive statistics.

	Mean	SD	McDonald's ω	Cronbach's α
Q2	2.282	1.415	0.7	0.701
Q3	2.018	1.75	0.717	0.705
Q4	2.782	0.98	0.731	0.722
Q5	2.064	1.442	0.721	0.709
Q6	1.509	1.339	0.728	0.714
Q7	2.445	1.506	0.737	0.727
Q8	1.727	1.196	0.734	0.725
Q9	1.8	1.501	0.705	0.697
Q10	2.164	1.784	0.738	0.727
Q11	1.818	0.988	0.721	0.71
Q12	2.2	1.841	0.681	0.694
Q13	1.691	1.519	0.703	0.698
Q14	1.6	1.416	0.732	0.721
Q15	1.436	1.253	0.722	0.709
Q16	2.455	1.282	0.71	0.708
Q17	2.391	1.348	0.7	0.701
Q18	1.1	0.301	0.731	0.723
Q19	3.327	1.853	0.696	0.698
Q20	1.609	0.49	0.733	0.723
Q21	1.327	0.94	0.729	0.718
Q22	1.627	1.226	0.728	0.719
Q23	2.809	1.758	0.731	0.72
Q24	1.518	1.139	0.728	0.715
Q25	1.818	1.342	0.731	0.719

Notably, item Q18 stands out with a mean of 1.1, suggesting a relatively low response value. Similarly, item Q15, with a mean of 1.436, represents another item with a relatively lower average response.

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 of 0.681 to 0.738, indicating a generally acceptable level of internal reliability.

Demographic information

Figure 2 provides insights into the participants' age distribution, revealing that 66% are below the age of 35 and include individuals from diverse age groups, encompassing both younger employees and those with more experience.

Furthermore, Figure 3 showcases the gender distribution of the participants, with 64% being male and 34% female. These percentages align with the official data reported by INEGI on February 20th, 2023, which indicates that 40% of the economically active population in the state of Guanajuato is female, while 60% is male.

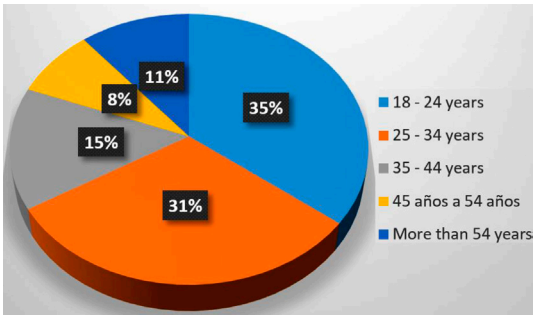

Figure 2. Demographic age.

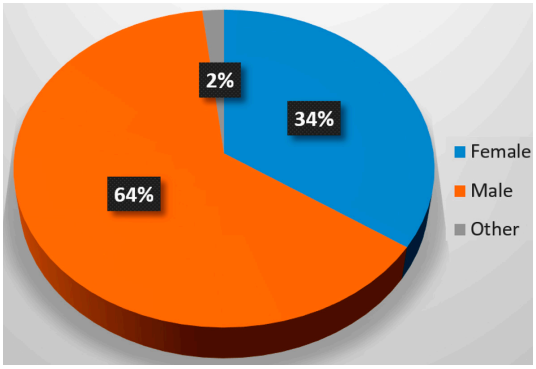

Figure 3. Demographic information by gender.

Regarding economic sectors, Figure 4 illustrates the breakdown of participants by their respective industries at the time of the survey. Notable portions of participants (63%) are employed in service companies, while 15% are engaged in wholesale trade.

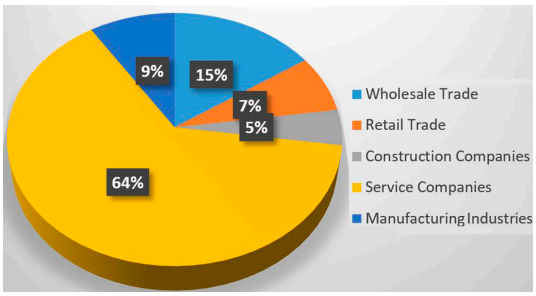

Figure 4. Demographic information by economic sectores.

Figure 5 highlights the participants' educational qualifications, indicating that 68% hold a bachelor's degree and 18% possess a master's degree. This data underscores the demand for highly qualified individuals within the city's companies, emphasizing the significance of advanced education in the workforce.

Security awareness gaps and potential risks in organizations

The analysis revealed important insights regarding the participants' awareness of security practices within their organizations. While a significant portion, 53.64% of the participants, recognized the presence of a dedicated security information department, areas of concern still need to be addressed (Figure 6).

Surprisingly, 10.91% of the participants indicated a lack of information, which poses a potential risk for their organizations. The fact that 35.45% of the participants were unaware of the existence of a security information department is equally alarming, as it represents a higher risk. These participants falsely believe they believe they receive information when, in reality, misinformation may occur.

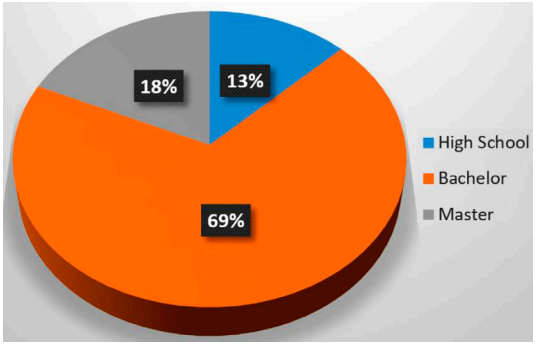

Figure 5. Demographic information by education.

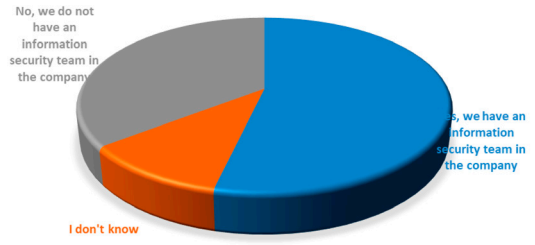

Figure 6. Information security department on organizations.

The findings further compound these concerns that 25.45% and 35.45% of the participants expressed uncertainty about whom to contact or how to identify a malware infection on their PCs. This lack of knowledge increases the likelihood of participants unknowingly using compromised devices, thus potentially exposing their organizations to further security breaches.

Lastly, it is troubling to note that 30.91% of the participants still need to configure automatic computer updates. This oversight leaves their systems vulnerable to known security vulnerabilities that could have been addressed through regular updates.

In light of these findings, organizations need to enhance security awareness and promote best practices among their employees. This includes providing comprehensive training, implementing robust security protocols, and fostering a culture of vigilance to mitigate risks and protect sensitive information effectively.

Social engineering risks on organizations

Social engineering poses a significant risk to every organization as it specifically targets users, making every employee vulnerable to becoming a victim or target. Within this context, it is crucial for all employees, from cleaners and maintenance staff to engineers and managers, to comprehend the risks associated with their responsibilities within the organization and the potential consequences that can impact the entire organization. Another significant issue is that 12.73% of the participants admitted to sharing passwords with their colleagues at work (Figure 7). This practice poses a substantial risk regarding social engineering and internal threats, making them easy targets for malicious actors.

Regarding attacks associated with email use, 41% of the participants mentioned opening email attachments when they recognized the sender's name or company without verifying their authenticity. This behavior is concerning because it exposes the organization to malware infections, data breaches, and unauthorized access to sensitive information. The previous results gain further significance when considering that 30% of the participants lack knowledge about phishing attacks and cannot identify them despite their prevalence before, during, and after the COVID-19 pandemic. This lack of

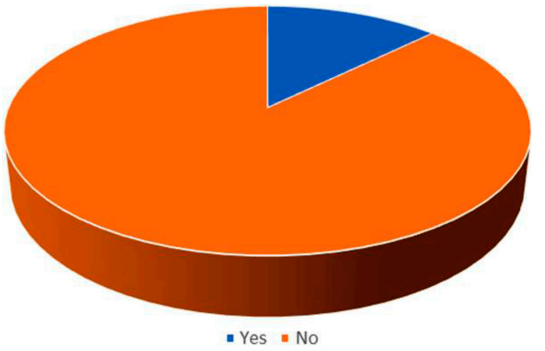

Figure 7. Percentage of users that share passwords.

awareness puts the organization at a higher risk of falling victim to sophisticated phishing schemes, which can potentially lead to significant financial and reputational damage.

Furthermore, when participants were asked whether they believed their computers held no value to hackers and thus were not targeted, 10.91% answered affirmatively. This misconception represents a significant risk to the organization as it demonstrates a lack of understanding about the potential impact of a compromised computer. Hackers can exploit seemingly insignificant devices to gain unauthorized access, launch further attacks, or use them as a stepping stone to infiltrate the organization's network, jeopardizing sensitive data, intellectual property, and critical systems.

Organizations must prioritize security awareness and education initiatives to ensure that all employees, regardless of their roles, have the knowledge and understanding to recognize and mitigate social engineering attacks, including:

- Promoting a culture of cybersecurity.
- Providing regular training sessions.
- Implementing robust policies and procedures to safeguard against these risks.

Inadequacy of communication on security policies

Figure 8 highlights a critical security issue from the perspective of organizations, specifically regarding the absence or inadequacy of security policies. Within this context, 30.91% of the participants reported that there are policies in place limiting their access to certain websites at work. Still, they must be made aware of these policies, revealing a significant internal communication gap or need for employee awareness regarding security policies.

More concerning is that 38.18% of the participants stated that their organizations have no security policies, leaving them vulnerable to various security risks and potential breaches. Furthermore, 39.09% of the participants indicated the absence of policies about adequately using the organization's email system. This lack of guidance and control over email usage increases the risk of data leakage, unauthorized access, and other security incidents.

A particularly alarming finding is that 51.82% of the participants mentioned that they could use their devices to store or transfer confidential company information, which poses a significant threat to the organization's data security, as it exposes sensitive information to potential loss, theft, or unauthorized sharing.

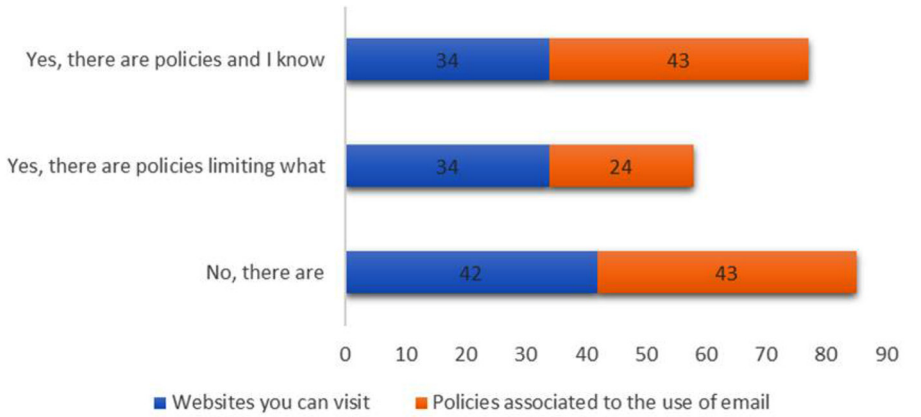

Figure 8. Absence of internal communication.

Lastly, 60.91% of the participants reported being free to download and install software from the internet on their work computers. This practice introduces additional risks, including the potential installation of malware or malicious programs that can compromise the organization's network and data integrity.

Overall, these findings underscore the pressing need for organizations to establish robust and comprehensive security policies to mitigate risks, enhance data protection, and foster a culture of security awareness among employees.

Risk level

To calculate the Individual's Risk Score (IRS) for each survey participant, we utilize equation (1), where X represents the numerical value associated with the response to each of the 24 questions based on [31].

$$IRS = \sum_{i=2}^{24} X_i \quad (1)$$

The risk level is subsequently determined by referring to Table 2.

Figure 9 shows the ISR obtained by each participant. It is important to mention that the risk score for all the participants is 47.5 which is aligned with the risk level of moderate.

From Figure 9, we conducted a more in-depth analysis that delves into the nuances of cybersecurity culture, considering factors such as age group, gender, and educational background among the participants. This meticulous examination aims to comprehensively understand how these demographic variables influence the overall cybersecurity mindset within the surveyed cohort. By scrutinizing the intersectionality of age, gender, and educational levels, we aim to uncover patterns and variations that may exist in the participants' approach toward cybersecurity. This granular analysis allows us to discern unique perspectives and potential correlations that might be masked in a broader examination.

Table 2. Individual's risk level.

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

As delineated in Figure 10, the IRS analysis among participants unfolds an insightful narrative when considering different age groups. Seven participants in the 18-24 age bracket demonstrate a commendable cybersecurity posture, categorized as Low Risk. However, a significant portion falls within the Moderate Risk level, signaling the need for targeted interventions to enhance awareness and best practices. Moreover, a notable number of individuals in this age range exhibit an Elevated Risk level, warranting attention to specific risk factors.

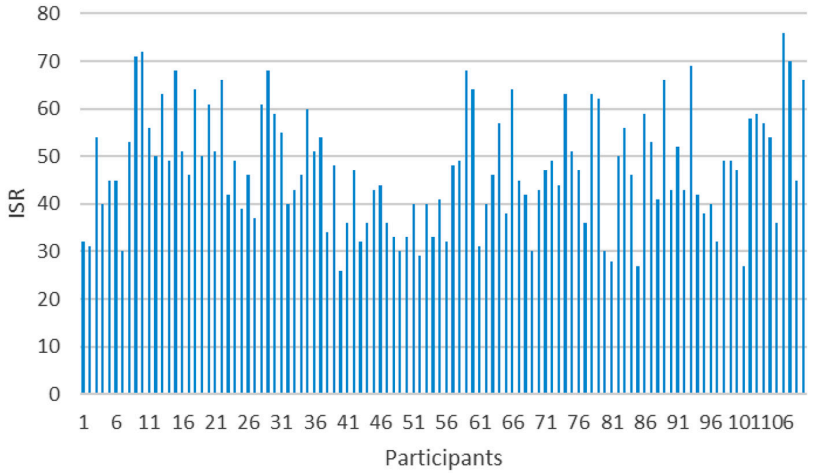

Figure 9. ISR by participants.

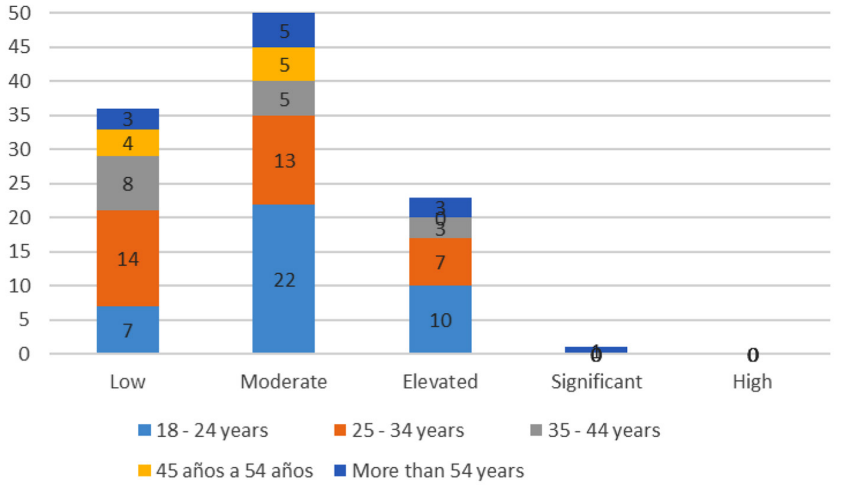

Figure 10. Risk level by age group.

Moving on to the 25-34 age group, 14 participants showcase a strong cybersecurity foundation, positioning them in the Low-Risk category. However, the presence of an Elevated Risk level among many underscores the importance of targeted interventions to address specific areas of concern.

Eight participants aged 35-44 exhibit a relatively low cybersecurity risk, categorized as Low Risk. However, Moderate Risk signals an opportunity for targeted training to enhance cybersecurity awareness, and an Elevated Risk level highlights areas for improvement in this age category.

In the 45-54 age group, a low cybersecurity risk is observed among four participants, categorized as Low Risk. Nevertheless, the combined presence of participants in both the Moderate and Elevated Risk categories suggests specific areas that may benefit from focused interventions.

Lastly, participants above 54 demonstrate a low cybersecurity risk, with three participants in the Low-Risk category. Moderate and Elevated Risk levels in this age group indicate an opportunity for targeted interventions to address factors contributing to elevated risk.

In conclusion, this age-based analysis unveils a diverse context of cybersecurity risk levels across different generational cohorts. This nuanced understanding facilitates the development of targeted interventions and educational programs tailored to the specific needs of each group, ultimately contributing to a more resilient cybersecurity culture within the surveyed population.

Examining the IRS in the context of gender-specific variations from the Employee Security Awareness Survey in Leon City yields insightful observations. This study, encompassing 110 participants, categorizes results into Low, Moderate, Elevated, Significant, and High-risk levels to provide a nuanced perspective on the reality of security awareness (Figure 11). The results among female participants, are noteworthy: eight individuals demonstrated a low-risk level, indicating robust adherence to security protocols. Nineteen females fell into the Moderate Risk category, suggesting a balanced security awareness level. Eleven females exhibited an Elevated Risk, pinpointing specific areas for targeted interventions. Importantly, no females were classified in the Significant or High-Risk categories, signifying a commendable overall security posture among female participants.

Among male participants, the data reveals that 28 individuals demonstrated a low-risk level, reflecting a solid adherence to security guidelines. Thirty males fell into the Moderate Risk category, indicating a moderate level of security awareness. Eleven males exhibited an Elevated Risk, signaling areas for improvement. Significantly, one male participant fell into the Significant Risk category, warranting immediate attention. No males were classified in the High-Risk category, underscoring a high-security awareness.

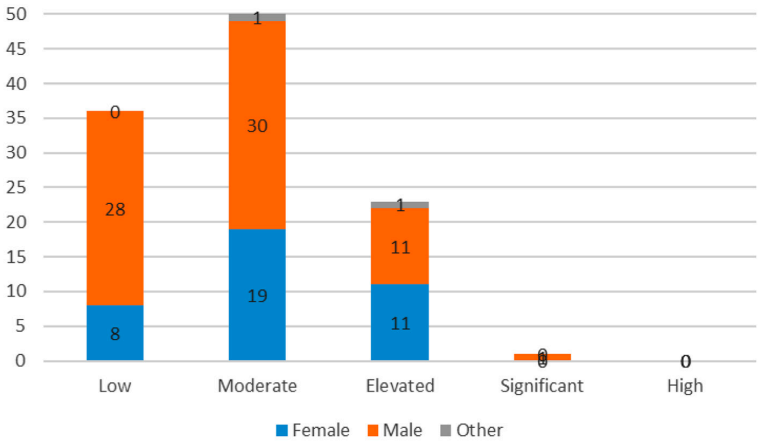

Figure 11. Risk level by gender.

In the "Other" category, one participant fell into the Moderate Risk range, while another exhibited an Elevated Risk. Importantly, no "Other" category participants were classified in the Significant or High-Risk categories.

Our results emphasize the importance of gender-inclusive security awareness initiatives. The absence of females in the Significant and High-Risk categories and the specific areas identified for improvement provide a solid foundation for tailoring training programs. Similarly, the results affirm the need for targeted interventions among participants in the "Other" category. This study contributes valuable insights into the gender-based variations in security awareness levels among employees in Leon City.

The detailed categorization of IRS results facilitates the development of customized training programs to address specific needs, ultimately enhancing the organization's overall security posture.

The analysis of ISR among 110 participants, categorized by their educational backgrounds in Figure 12, provides a new view of the cybersecurity culture within different academic cohorts. Participants with a high school education show commendable awareness, with three individuals falling into the Low-Risk category. However, a notable proportion falls within the Moderate and Elevated Risk levels, indicating areas for targeted interventions to enhance awareness and practices. Bachelor's degree holders demonstrate a robust understanding of cybersecurity

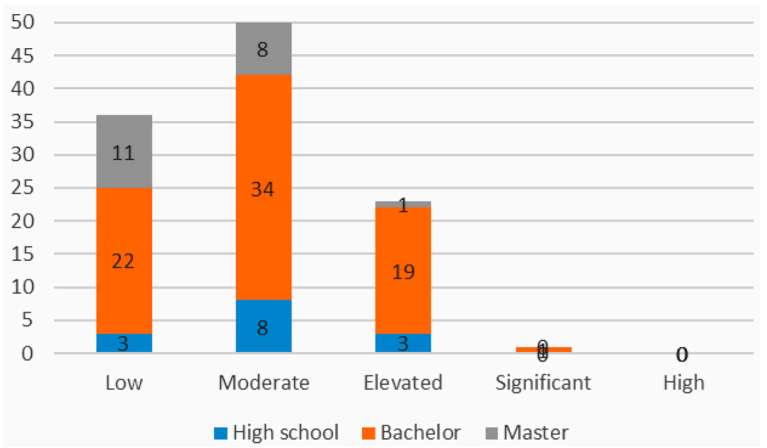

Figure 12. Risk level by age group.

practices, with 22 participants categorized as low-risk. However, the prevalence of Moderate and Elevated Risk levels among this cohort emphasizes the need for targeted training to address specific areas of improvement. Those with a master's degree showcase a generally strong cybersecurity culture, with 11 individuals in the Low-Risk category. The presence of both Moderate and Elevated Risk levels among master's degree holders suggests areas for further enhancement. This detailed analysis provides insights into the cybersecurity culture across educational backgrounds, guiding the development of tailored educational programs to foster a more resilient cybersecurity culture among participants.

CONCLUSIONS

This study analyzed diverse factors contributing to cybersecurity culture among employees within organizational settings. A notable revelation is the visibility of age as a significant factor, challenging the prevailing assumption that older employees possess diminished technological proficiency and are more susceptible to cybersecurity threats. Consequently, the study underscores the imperative of inclusive cybersecurity training programs tailored to accommodate individuals across various age cohorts.

Contrary to expectations, gender was found to be inconsequential in influencing employees' cybersecurity risk levels. This observation underscores organizations' need to adopt gender-neutral approaches in crafting cybersecurity training and awareness initiatives, ensuring their effectiveness across diverse gender demographics.

Moreover, the study elucidates the positive correlation between higher educational attainment, heightened cybersecurity awareness, threat identification proficiency, and employee adherence to security policies. Accordingly, organizations are encouraged to tailor their cybersecurity training programs to align with disparate educational backgrounds, ensuring comprehensive coverage and effective risk mitigation strategies. The importance of cybersecurity teams within organizations in improving the overall cybersecurity culture is being investigated for future work. The main limitations are: Firstly, the relatively small sample size of 110 surveys and the use of self-reported data may impact the generalizability and accuracy of the findings. Secondly, the study's focus on León City limits its applicability to the broader diversity within México.

REFERENCES

[1] L.F. Ribas Monteiro, Y.R. Rodrigues, and A.C. Zambroni de Souza, "Cybersecurity in Cyber-Physical Power Systems," *Energies*, vol. 16, no. 12, p. 4556, 2023, doi: 10.3390/en16124556.

[2] A. López Martínez, M. Gil Pérez, and A. Ruiz-Martínez, "A Comprehensive Review of the State-of-the-Art on Security and Privacy Issues in Healthcare," *ACM Computing Surveys*, vol. 55, no. 12, pp. 1-38, 2023, doi: 10.1145/3571156.

[3] M.M. Leal and P. Musgrave, "Backwards from zero: How the U.S. public evaluates the use of zero-day vulnerabilities in cybersecurity," *Contemporary Security Policy*, vol. 44, no. 3, pp. 437-461, 2023, doi: 10.1080/13523260.2023.2216112.

[4] A. Bahl, A. Sharma, and M.R. Asghar, "Vulnerability disclosure and cybersecurity awareness campaigns on twitter during COVID-19," *Security and Privacy*, vol. 4, no. 6, p. e180, 2021, doi: 10.1002/spy2.180.

[5] F. Gioulekas *et al.*, "A cybersecurity culture survey targeting healthcare critical infrastructures," *Healthcare*, vol. 10, no. 2, p. 327, 2022, doi: 10.3390/healthcare10020327.

[6] D. Du, M. Zhu, X. Li, M. Fei, S. Bu, L. Wu, and K. Li, "A Review on cybersecurity analysis, attack detection, and attack defense methods in cyber-physical power systems," *Journal of Modern Power Systems and Clean Energy*, vol. 11, no. 3, pp. 727-743, 2023, doi: 10.35833/MPCE.2021.000604.

[7] A. Georgiadou, A. Michalitsi-Psarrou, and D. Askounis, "A security awareness and competency evaluation in the energy sector," *Computers & Security*, vol. 129, p. 103199, 2023, doi: 10.1016/j.cose.2023.103199.

[8] K. Renaud and J. Ophoff, "A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs," *Organizational Cybersecurity Journal: Practice, Process and People*, vol. 1, no. 1, pp. 24-46, 2021, doi: 10.1108/OCJ-03-2021-0004.

[9] M. Alsharif, S. Mishra, and M. AlShehri, "Impact of human vulnerabilities on cybersecurity," *CSSE*, vol. 40, no. 3, pp. 1153-1166, 2021, doi: 10.32604/csse.2022.019938.

[10] C. Nobles, "Botching human factors in cybersecurity in business organizations," *HOLISTICA - Journal of Business and Public Administration*, vol. 9, no. 3, pp. 71-88, 2018, doi: 10.2478/hjbpa-2018-0024.

[11] N. Gcaza, R. von Solms, M.M. Grobler, and J.J. van Vuuren, "A general morphological analysis: delineating a cyber-security culture," *Information & Computer Security*, vol. 25, no. 3, pp. 259-278, 2017, doi: 10.1108/ICS-12-2015-0046.

[12] G.P.S. Tejay and Z.A. Mohammed, "Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective," *Information & Management*, vol. 60, no. 3, p. 103751, 2023, doi: 10.1016/j.im.2022.103751.

[13] J. Shires, "Cyber-noir: Cybersecurity and popular culture," *Contemporary Security Policy*, vol. 41, no. 1, pp. 82-107, 2020, doi: 10.1080/13523260.2019.1670006.

[14] B. Uchendu, J.R.C. Nurse, M. Bada, and S. Furnell, "Developing a cyber security culture: Current practices and future needs," *Computers & Security*, vol. 109, p. 102387, 2021, doi: 10.1016/j.cose.2021.102387.

[15] K. Ruan, J. Carthy, T. Kechadi, and I. Baggili, "Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results," *Digital Investigation*, vol. 10, no. 1, pp. 34-43, 2013, doi: 10.1016/j.diin.2013.02.004.

[16] A. Georgiadou, S. Mouzakitis, and D. Askounis, "Working from home during COVID-19 crisis: a cyber security culture assessment survey," *Security Journal*, vol. 35, no. 2, pp. 486-505, 2022, doi: 10.1057/s41284-021-00286-2.

[17] O. Ogbanufe, R.E. Crossler, and D. Biros, "Exploring stewardship: A precursor to voluntary security behaviors," *Computers & Security*, vol. 109, p. 102397, 2021, doi: 10.1016/j.cose.2021.102397.

[18] Secureops, "SANS - The Five Most Dangerous Cyberattacks". secureops.com. https://secureops.com/blog/5-dangerous-attacks/ (accessed Jun. 17, 2023).

[19] N. Baltagi, "Understanding cyberattacks and the threat landscape with SANS Institute". gulfnews.com. https://gulfnews.com/business/understanding-cyberattacks-and-the-threat-landscape-with-sans-institute-1.1685582002052 (accessed Jun. 3, 2023).

[20] OWASP, "OWASP Top Ten | OWASP Foundation". owasp.org. 2023. https://owasp.org/www-project-top-ten/ (accessed Mar. 17, 2023).

[21] N. Tariq, "Impact of cyberattacks on financial institutions," *Journal of Internet Banking and Commerce*, vol. 23, no. 2, p. 1-11, 2018.

[22] J.F. Carías, M.R.S. Borges, L. Labaka, S. Arrizabalaga, and J. Hernantes, "Systematic Approach to Cyber Resilience Operationalization in SMEs," *IEEE Access*, vol. 8, pp. 174200-174221, 2020, doi: 10.1109/ACCESS.2020.3026063.

[23] Z.M. King, D.S. Henshel, L. Flora, M.G. Cains, B. Hoffman, and C. Sample, "Characterizing and Measuring Maliciousness for Cybersecurity Risk Assessment," *Frontiers in Psychology,* vol. 9, p. 39, 2018.

[24] S. Kraemer and P. Carayon, "A Human Factors Vulnerability Evaluation Method for Computer and Information Security," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 47, no. 12, pp. 1389-1393, 2003, doi: 10.1177/154193120304701202.

[25] U.D. Ani, H. He, and A. Tiwari, "Human factor security: evaluating the cybersecurity capacity of the industrial workforce," *Journal of Systems and Information Technology*, vol. 21, no. 1, pp. 2-35, 2019, doi: 10.1108/JSIT-02-2018-0028.

[26] A. Nikpour, "The impact of organizational culture on organizational performance: The mediating role of employee's organizational commitment," *International Journal of Organizational Leadership,* vol. 6, no. 1, pp. 65-72, 2017, doi: 10.33844/ijol.2017.60432.

[27] N. Nazir and D.S. Zamir, "Impact of Organizational Culture on Employee's Performance," *Industrial Engineering Letters*, vol. 5, no. 9, pp. 31-37, 2015.

[28] M. Evans, L.A. Maglaras, Y. He, and H. Janicke, "Human behaviour as an aspect

of cybersecurity assurance," *Security and Communication Networks*, vol. 9, no. 17, p. 4667-4679, 2016. doi: 10.1002/sec.1657.

[29] A. Da Veiga, "A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument," in *2016 SAI Computing Conference (SAI)*, 2016, pp. 1006-1015, doi: 10.1109/SAI.2016.7556102.

[30] N. Gcaza and R. von Solms, "A strategy for a cybersecurity culture: A South African perspective," *The Electronic Journal of Information Systems in Developing Countries*, vol. 80, no. 1, pp. 1-17, 2017, doi: 10.1002/j.1681-4835.2017.tb00590.x.

[31] F.J. García Arellano, T.E. Venegas Chávez, S. Olivares-Bautista, and R. Martínez-Peláez, "Navegando por los desafíos de la ciberseguridad: Un estudio sobre la concientización de los empleados en organizaciones privadas", *Tecnotrend*, no. 16, pp. 1-16, 2024.

[32] T. Bond, "Employee Security Awareness Survey," 2012.

[33] N. Ahmed, U. Kulsum, I. Bin Azad, A.S.Z. Momtaz, M.E. Haque, and M.S. Rahman, "Cybersecurity awareness survey: An analysis from Bangladesh perspective," in *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*, 2017, pp. 788-791, doi: 10.1109/R10-HTC.2017.8289074.

[34] W. Rodgers, E. Alhendi, and F. Xie, "The impact of foreignness on the compliance with cybersecurity controls," *Journal of World Business*, vol. 54, no. 6, p. 101012, 2019, doi: 10.1016/j.jwb.2019.101012.

[35] A. Onumo, I. Ullah-Awan, and A. Cullen, "Assessing the Moderating Effect of Security Technologies on Employees Compliance with Cybersecurity Control Procedures," *ACM Transactions on Management Information Systems*, vol. 12, no. 2, pp. 1-29, 2021, doi: 10.1145/3424282.

[36] S. Allam, S.V. Flowerday, and E. Flowerday, "Smartphone information security awareness: A victim of operational pressures," *Computers & Security*, vol. 42, pp. 56-65, 2014, doi: 10.1016/j.cose.2014.01.005.

[37] M.A. Omer, A.A. Yazdeen, H.S. Malallah, and L.M. Abdulrahman, "A survey on cloud security: concepts, types, limitations, and challenges," *Journal of Applied Science and Technology Trends*, vol. 3, no. 2, pp. 101-111, 2022, doi: 10.38094/jastt301137.