The Role of Cybersecurity in Information Systems in Organizations: a systematic literature review

Eduardo Santos, Gonçalo Passos, Pedro Bastos, and Pedro Sobral, DETI UA

***Abstract*—This paper presents a systematic literature review examining the role of cybersecurity in information systems in organizations. The review presents an in-depth analysis of ten studies published between 2017 and 2023 and aims to identify the significance and role of cybersecurity in information systems within organizations. This systematic review was carried out from relevant research using the Scopus database.**

The analysed documents reveal an increasing trend in cyber-attacks, attributing this rise to the growing permeability of organizational boundaries in the digital age. They underscore the importance of robust systems, such as Supervisory Control and Data Acquisition (SCADA), in maintaining real-time control and monitoring of critical infrastructures.

The review also highlights the critical role of cybersecurity awareness within organizations. It emphasizes the need for a strong security culture, underpinned by continuous education and training, to enhance the overall resilience of organizations against cyber threats.

The rapid pace of digital modernization and its implications for cybersecurity is another key theme. The documents point to the escalating complexity of cybersecurity threats in the wake of digital transformation and stress the importance of regular security audits in managing these risks effectively.

The role of top management and their influence on cybersecurity practices is also explored. The documents suggest that those in the highest positions, including the Chief Information Officer (CIO), should take a proactive role in integrating cybersecurity into the broader business strategy.

In conclusion, this review provides a comprehensive understanding of the multifaceted role of cybersecurity in information systems within organizations. It also identifies potential avenues for future research, emphasizing the need for empirical investigations, exploration of cultural influences, and case studies focusing on security success outcomes.

***Index Terms*—Cybersecurity, Information Systems, Security Of Data, LaTeX, Security Systems, Data Privacy.**

I. Introduction

CYBERSECURITY has become a major concern for businesses all over the world in the modern digital era. The potential for cyber threats has exploded as digital technologies continue to develop and permeate every aspect of organizational operations. The security and integrity of information systems within organizations are seriously at risk from these threats, which include data breaches and sophisticated cyberattacks.

The cybersecurity landscape has changed significantly over the last few years. New opportunities for efficiency and innovation have been created by the emergence of technologies like cloud computing, AI, and the Internet of Things (IoT). The task of securing information systems has become more difficult as a result of the new vulnerabilities and attack vectors that have been brought about by these developments.

The nature of cyber threats has also changed, in addition to technological advancements. Cybercriminals are becoming more skilled, using cutting-edge methods, and continuously modifying security precautions. The cybersecurity environment has become even more complicated as a result of state-sponsored cyberattacks and cyberespionage.

Additionally, the challenges associated with cybersecurity have been exacerbated by the rise of remote work in response to the global pandemic. In order to quickly adapt to a distributed workforce, organizations frequently lacked the necessary security infrastructure, making them more susceptible to cyber-attacks.

Understanding the function of cybersecurity in information systems in this context is crucial for organizations on a strategic level. It requires a comprehensive strategy that takes organizational culture, human factors, and strategic considerations into account in addition to technological measures.

Using the most recent findings and advancements in the field, this paper aims to present a thorough overview of the current state of cybersecurity in information systems within organizations. It will go into depth on important subjects like the causes of the rise in cyberattacks, the value of cybersecurity awareness within organizations, the effects of digital modernization on cybersecurity, and the responsibility of top management in preventing and managing security breaches.

The importance of cybersecurity in information systems will undoubtedly continue to develop as we move through the digital transformation era, demanding ongoing research, vigilance, and adaptation.

II. Methodology

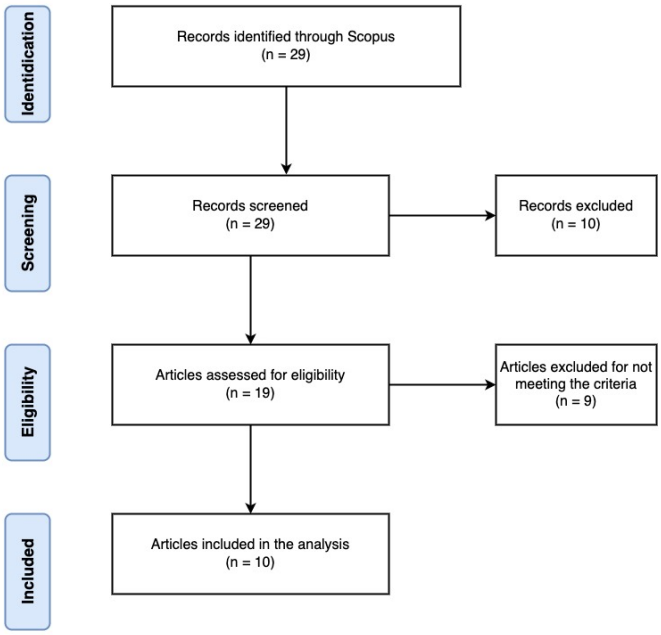
In this study, a systematic literature review is conducted to obtain a comprehensive understanding of the current state-of-the-art regarding the role of Cybersecurity in Information Systems in Organizations. The primary goal of this review is to evaluate the published articles in this field and gain insights into the studies' objectives, data collection and analysis methods carried out, as well as the key findings. This section provides a detailed account of the methodology employed in conducting the literature review, including article selection and analysis processes, and presents the thematic areas covered by the selected articles.

A. Selection of the articles

The Scopus database was used to search and find the publications intended for this review. The query (”cybersecurity” AND ”role” AND ”Information Systems” AND

"Organizations") with the time period between 2017 and 2023 returned 29 documents, where 10 were excluded for not being within the scope of this literature review. The abstract and introduction of the 19 articles were closely analysed and we concluded that 9 of them had a small substantial matter for this study case and were eliminated. With that in mind, 10 articles were determined relevant and included in this literature review. This process is presented in Figure 1.

Fig. 1. Article selection process



B. Data analysis

To successfully understand each article and how they can correlate with each other, we were able to group them into 4 main topics (Table I).

TABLE I
TOPICS AND ARTICLES

Topics	Publications
Cyber Security Awareness in Organizations	[6], [2]
Reasons for Increase in Cyber-attacks	[5][13], [14]
Importance of the Highest Positions in the Prevention and Management of Security Breaches	[8], [9], [10]
The Role of External Auditors and IT Modernization in Reducing Cybersecurity Risks	[11], [12]

C. Article analysis

The interest in the cybersecurity within the organizations is growing at a faster rate than ever. More and more organizations have been spending effort, time and money into this field and its growth reflects on the investigation carried in it. For that reason, the best and most relevant articles found in this area are from the last 4-5 years. Figure 2 shows the distribution of the included articles in each year.

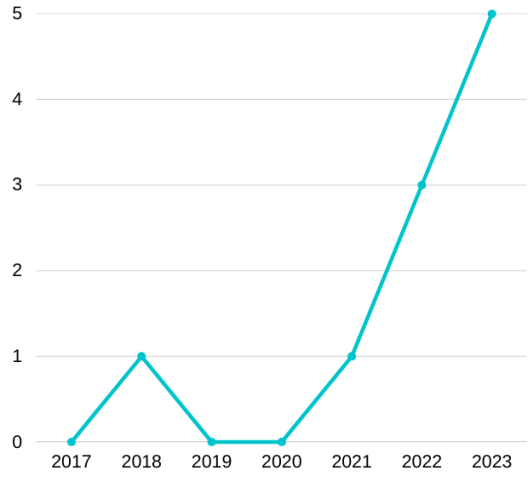


Fig. 2. Article distribution

III. Cyber Security Awareness in Organizations

In the modern era, the Internet has become a staple for a multitude of activities, including e-commerce and online banking. As a result, cybersecurity has emerged as a critical issue, particularly for the financial sector, which is frequently targeted by cyber threats [2], although many other sectors suffer from this problem.

These dangers can manifest in a variety of ways, such as email phishing, ransomware, malware, and denial-of-service (DoS) attacks, etc., and they have a wide range of effects on organizations. However, if users are aware of cybersecurity issues, the risks posed by these threats can be reduced. According to the Information Security Awareness (ISA) model, a number of personal factors, such as cybersecurity training, educational background, work experience, field of study, gender, age, training, and place of residence, have an impact on this awareness [2].

In order to protect users' assets and the environment of the organization, cybersecurity encompasses a range of best practices, concepts, policies, assurances, guidelines, safeguards, actions, risk management strategies, training, tools, and technologies. Any information found in the cyber environment, including networked devices, infrastructure, telecommunications systems, services, and applications, can be included in these assets. They must be protected based on the CIA's three main goals of confidentiality (C), integrity (I), and availability (A).

Understanding security threats and taking the necessary precautions to reduce risks is known as cybersecurity awareness (CSA). It is essential to give CSA training to people who work directly with information systems. This instruction can

improve both the organization's and the individuals' level of protection.

It is argued that developing an information security culture will lead to a secure organization. Members of the organization act as its first line of defense in this situation. Employees frequently fall victim to social engineering techniques employed by hackers, or they act carelessly endangering the security of crucial information assets within an organization [7].

In addition to cybersecurity, information security involves data protection measures, such as the General Data Protection Regulation (GDPR), which safeguard sensitive data from unauthorized access, exposure, or theft.

A number of demographic factors, such as gender, age, nationality, field of study, work experience, and training, affect cybersecurity awareness. For instance, it's been discovered that gender can influence security self-efficacy, prior experience, and computer skills. It's also been discovered that years of computer usage or experience, as well as gender, significantly influence the rate of phishing detection [2].

IV. Reasons for Increase in Cyber-attacks

Cyber attacks are increasingly being talked about, and the consequences of these attacks are being recognized as extremely harmful. Every day, more and more devices are being connected to the Internet, and this trend is visible across various sectors of the industry and essential services. The increasing digitization of systems and services in areas like health information systems, Industrial Internet of Things, and remote work creates new cyberattack surfaces requiring robust and evolving cybersecurity measures, from all the actors. The main rule/concept to reduce cybercrime in all these sectors goes through developing comprehensive cybersecurity policies and implementing both basic and advanced security controls.

Healthcare organizations needs a lot of security in the virtual layer, the concept of privacy in this sector is a main character, and is very important to have the right security policies to protect the sensitive user data. It is important to emphasize the regular compliance checks with security standards, in order to understand the latest regulations that must be applied in health information systems, in order to reduce (at least try) the vulnerabilities. The greatest vulnerability in healthcare organizations is the human factor, emphasizing the need for more support for healthcare cybersecurity professionals and their cybersecurity programs [4].

In the context of the Industrial Internet of Things (IIoT), sectors such as transport, energy, and industry face unique security threats. The integration of new internet-connected devices into critical infrastructure operations is creating new attack surfaces that can expose critical functionalities to cyberattacks with severe consequences. Given all these attacks, new technologies and cybersecurity methods will be necessary to address the challenging technical aspect of operating IIoT equipment securely. A critical insight is the potential for systemic risk, where a security breach in one part of the IIoT can potentially affect other parts of the system, causing widespread disruptions or even physical damage [13].

As the number of end-users (largely remote workers) connecting remotely to a server or network increased very significantly in the last years, so more people are exposed to cyberattacks every day and the attack surface inevitably expands. Some of the best practices for remote work are: the use of various communication channels, regular training sessions on cybersecurity awareness, and the use of technological solutions such as endpoint security software like VPNs and firewalls. Other good practices to maintain cybersecurity awareness are: having strong and unique passwords, keeping the software and operating systems updated, being wary of phishing emails and suspicious links, and avoiding the use of public Wi-Fi for work-related activities [14].

In our increasingly interconnected world, the constant influx of devices connecting to the internet has resulted in a higher number of vulnerabilities within networks. The primary objective remains addressing existing vulnerabilities and providing knowledge on mitigating potential risks. The three topics mentioned above emphasize the necessity of a comprehensive cybersecurity approach across all sectors and modes of operation, emphasizing the importance of robust and adaptable security policies. This approach recognizes the ever-changing nature of cybersecurity threats and the need to continually update defenses. By prioritizing comprehensive training and awareness programs, individuals can acquire the skills needed to identify and respond to emerging cyber threats effectively. Moreover, the integration of advanced technological solutions is essential for proactive threat detection and neutralization. By adopting this comprehensive approach, we can create a safer digital environment, protecting critical information and infrastructure in our interconnected world.

V. Importance of the Highest Positions in the Prevention and Management of Security Breaches

An essential component of cybersecurity governance is the significance of the top positions inside businesses, especially top management teams (TMTs), in the prevention and management of security breaches.

It is important to have information security risk assessments (ISRAs) in the wake of cybersecurity breaches, as is the mediating function of TMT attention to cybersecurity, as introduced by [9] . It emphasizes how robust responses to violations must take into account both internal and external factors. The cost of a breach affects the TMT's attention to cybersecurity, and higher breach costs cause more attention to be paid to security because of the failure to ensure security and the obligation to stakeholders. The study emphasizes the connection between breach costs, TMT security awareness, and the choice to do an ISRA. The findings highlight the significance of TMTs in setting cybersecurity as a top priority and devoting funds for risk analysis and management.

[10] takes a strategic leadership stance and focuses on digital firms' cyber-resiliency. It draws attention to the negative effects of cyberattacks on reputation, data loss, and knowledge loss. The paper stresses how little is known empirically about how strategic leaders influence and support cybersecurity strategies. The study outlines recommended practices for achieving cyber-resiliency through exploratory interviews with

Chief Information Officers (CIOs), Chief Security Information Officers (CSIOs), and Chief Technology Officers (CTOs). Making cyber-resilience a crucial organizational competency, comprehending the ecosystem and interactions with partners and suppliers, developing governance frameworks, and allocating responsibility for the success of cybersecurity strategies are some examples of these techniques. The conclusions of this article emphasize the critical part that strategic leaders play in promoting cybersecurity measures and incorporating them into business culture.

As emphasized by [8], it is important to build formal leadership development programs that are specifically designed for cybersecurity and information technology (IT) professionals. It emphasizes how professionals' capacity to effectively manage risks, lead teams, and make strategic decisions in line with organizational goals is hampered by the way traditional technical training programs frequently overlook the development of leadership qualities. In the context of cybersecurity and IT, the paper makes the case for the introduction of formal leadership development programs that improve abilities including strategic thinking, communication, team management, problem-solving, and decision-making. These courses ought to include the particular difficulties faced by cybersecurity and IT workers, such as the requirement for constant innovation and adaptability in the face of increasing security threats. Organizations may improve their entire cybersecurity posture, promote collaboration between technical and non-technical teams, and establish a culture that appreciates technical expertise and effective leadership by investing in the development of cybersecurity and IT leaders.

Overall, the three papers offer insightful information about the significance of the top positions inside firms in managing and preventing security breaches. The development of leadership skills among cybersecurity and IT workers, strategic leaders' integration of cybersecurity strategies into organizational strategies, and TMT attention to cybersecurity are crucial to effectively tackling cybersecurity concerns. For effective cybersecurity governance, risk assessment, and risk management techniques, it is essential to comprehend and utilize the role of senior positions in firms.

VI. The Role of External Auditors and IT modernization in reducing cybersecurity risks

A. Legacy Systems vs. Cloud Systems

Within the common opinion of IT specialists, there is still belief in the "security-by-antiquity" notion for big organizations and companies. That is the idea that keeping the old Legacy Systems instead of changing to a modern system is beneficial and reduces the risk of cyber-attacks. As it is mentioned in the article [11] in the first hypothesis studied, people argue that:

- limited accessibility to Legacy Systems reduces their vulnerability;
- the lack of documentation and outdated tools make legacy systems less visible and limit the capabilities of likely offenders.

On the other hand, the modernization and migration to the cloud has its own advantages [11], (Hypothesis 2):

- cloud vendors have more resources and capabilities to provide effective protection compared to in-house legacy systems.
- standardization of IT interfaces in cloud migration reduces target accessibility and enables more effective security governance.
- cloud options attract and retain top security talent, offering better protection against evolving security threats.
- migration to the cloud involves modernization and standardization, decreasing target accessibility and improving security.

Overall, the study of both cases is performed in the article [11].

B. External Auditors

Usually, external auditors don't have digital capability when performing financial reporting. The article [12] studies the relationships between the digital innovation, digital capability of auditors, their effort, performance and risk. Over the years, they have improved and transformed, being familiar to the use of IT.

C. Reducing cybersecurity risks

Overall, the digital modernization, either in the systems themselves [11] or in the audit process [12], is shown to be beneficial to reducing risks to the organization's private data.

The study in [11] focuses on U.S. federal agencies, analysing the relation between security incidents and IT modernization, cloud computing spending, etc.

The results clearly state that a higher proportion of Legacy IT systems is associated with more security incidents in federal agencies and that migration to cloud based systems mitigate security risks.

It also shows that a smaller increase in the cloud budget leads to a larger decrease in security incidents. Not only breaches, but also usage and policy violation incidents.

Bridging this results from [11] with [12], we can correlate that, generally, the digital innovation leads to better security management, resulting in less security breaches.

Besides that, the longer the tenure of IT employees, the more frequent security breaches occur, while more educated IT workers experience fewer improper use incidents [11]. Nowadays, auditors collaborate with IT teams to provide more competent and reliable information through system applications. The greater the level of awareness possessed by the auditor, who plays a vital role in safeguarding data security by enhancing cybersecurity in the business infrastructure, the fewer security breaches occur [12].

As emphasized by [12], the significance of auditors understanding technological advancements at client companies is crucial to enhance audit implementation and uncover hidden findings for users of financial statements. that leads to higher security and less probability of breaches. Combining that with the IT modernization and cloud migration mentioned in [11], cybersecurity risks are considerably lower and more predictable and avoidable.

VII. Conclusion

In the current digital era, cybersecurity has grown to be a major concern, and organizations are at serious risk from a variety of cyber threats. However, raising users' awareness of cybersecurity issues can reduce these risks. The degree to which a person is aware of cybersecurity issues depends on a variety of factors, including training, education, experience, and personal background. For the purpose of safeguarding resources and preserving the confidentiality, integrity, and accessibility of information, best practices, policies, and technologies must be implemented.

Protecting sensitive data also requires fostering an information security culture within organizations and abiding by data protection laws like GDPR.

In general, security risks are much lower when modern solutions are applied. As shown before, cloud migration is crucial in a system to reduce breaches. Besides that, modernization is not only a positive solution within the system itself, but also in people. The role of external auditors is important in the sense that an updated, technologically advanced and careful auditor can prevent mistakes from the inside out of an organization.

References

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.

[2] Therdpong Daengsi, Pongpisit Wuttidittachotti, Phisit Pornpongtechavanich, and Nathaporn Utakrit *A comparative study of cybersecurity awareness on phishing among employees from different departments in an organization*, 2021.

[3] Muyowa Mutemwa, Jabu Mtsweni, and Lukhanyo Zimba, *Integrating a security operations centre with an organization's existing procedures, policies and information technology systems*, 2019.

[4] Margarida G.M. S. Cardoso, Rosário D. Laureano, and Carlos Serrão, *Cybersecurity culture in Portuguese organizations: an exploratory analysis*, 2017.

[5] Ahmad Mustafa Mohamad Al-Aboosi, Siti Norul Huda Sheikh Abdullah, Mohd Zamri Murah, and Ghassan Saleh ALDharhanio, *Cybersecurity Trends in Health Information Systems*, 2022.

[6] Tejay, G. P. S., & Mohammed, Z. A., *Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective*, 2023.

[7] Kure HI, Islam S, Mouratidis H., *An integrated cyber security risk management framework and risk predication for the critical infrastructure protection*, 2022.

[8] Burrell,D. N. and Aridi,A. S. and Nobles,C. *The critical need for formal leadership development programs for cybersecurity and information technology professionals.*, 2018.

[9] Faheem Ahmed Shaikh, Mikko Siponen, *Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity*, 2023.

[10] Loonam, J., Zwiegelaar, J., Kumar, V., Booth, C., *Cyber-resiliency for digital enterprises: A strategic leadership perspective. IEEE Transactions on Engineering Management*, 2022.

[11] Min-Seok Pang, Hüseyin Tanriverdi, *Strategic roles of IT modernization and cloud migration in reducing cybersecurity risks of organizations: The case of U.S. federal government*, 2022.

[12] Yohannes Kurniawan, Archie Nathanael Mulyawan, *The Role of External Auditors in Improving Cybersecurity of the Companies through Internal Control in Financial Reporting*, 2022.

[13] Louise Axon, Katherine Fletcher, Arianna Schuler, Marcel S., Robert Hannigan, Ali El Kaafarani, Michael Goldsmith, Sadie Creese, *Emerging Cybersecurity Capability Gaps in the Industrial Internet of Things: Overview and Research Agenda*, 2022

[14] Joseph K. Nwankpa, Pratim Milton Datta, *Remote vigilance: The roles of cyber awareness and cybersecurity policies among remote workers*, 2023

[15] John Loonam, Jeremy Zwiegelaar, Vikas Kumar, Charles Booth, *Cyber-Resiliency for Digital Enterprises: A Strategic Leadership Perspective* , 2023