SEVEN
publicações acadêmicas

CYBERSECURITY AND ATTACK RESISTANCE IN A CONNECTED WORLD

Hermenegildo Woropo Albino Paiva[1], José Gelson Gonçalves [2]

ABSTRACT

In response to the increasing digitalization that permeates social and organizational processes, this study proposes to investigate the challenges and strategies inherent to cybersecurity in a global context increasingly vulnerable to digital risks. The central objective is to analyze contemporary cyber threats, with particular emphasis on the vulnerability of critical infrastructures and the effectiveness of mitigation practices implemented by organizations in both the public and private sectors. To achieve this objective, the methodology adopted consisted of a comprehensive review of the existing literature, through which scientific articles, relevant institutional reports, and specialized technical documents, published in the period between 2018 and 2024, were examined. Thorough analysis of these materials revealed a significant increase in not only the frequency of cyberattacks, but also their sophistication, driven largely by the rise of organized cybercrime and the spread of the practice of "Cybercrime-as-a-Service." The main conclusion of the study points to the urgent need for an integrated and holistic approach to cybersecurity, which combines solid and transparent governance, an organizational culture intrinsically focused on information security, the strategic use of advanced technologies, such as SIEM (Security Information and Event Management) and SOCs (Security Operations Centers), and strict compliance with relevant standards and legislation, such as the General Data Protection Law (LGPD). The study emphasizes that only with the adoption of this systemic and comprehensive vision will it be possible to ensure the resilience and sustainability of organizations in an increasingly challenging digital environment prone to cyberattacks.

Keywords: Security. Internet. Threats.

[1] Master's student in Computer Science. Universidade Federal de Lavras.
E-mail: hermenegildo.paiva@estudante.ufla.br
[2] Master's student in Computer Science. Universidade Federal de Lavras.
E-mail: jose.goncalves1@estudante.ufla.br

1 INTRODUCTION

Digital transformation has intensely shaped contemporary society. Connectivity, previously restricted to computers and local networks, today permeates mobile devices, smart home appliances, transportation systems, hospitals, and critical infrastructure. With the exponential growth of the Internet of Things (IoT), artificial intelligence (AI), and cloud computing, the exposure of networks and systems to cyberattacks has increased significantly (Abreu; Nascimento, 2018).

In this scenario, cybersecurity emerges as an essential pillar to ensure the integrity and proper functioning of public and private services. The growing digitization of human activities makes data a high-value resource, the leakage or alteration of which can lead to serious financial, social, and even political consequences (Barbosa; Mattos, 2021). Governments, businesses, and citizens have come to rely on information security to ensure their operations and privacy in a complex digital ecosystem.

For Aguiar (2021), cyberwarfare and cyberterrorism have gained prominence in international relations, demonstrating that digital security is no longer an exclusively technical concern, but also geopolitical. Therefore, understanding the fundamentals of information security is essential to develop effective protection strategies.

Cybersecurity is composed of a set of practices, technologies, and policies aimed at protecting computer systems against unauthorized access, malicious attacks, technical failures, and human errors (Brandão; Reis, 2019). The objective is to preserve the integrity, confidentiality and availability of information.

The era of hyperconnectivity and digital transformation has brought significant advances in efficiency, automation, and social interaction. However, these advances have also dramatically expanded the surface of exposure to cyber risks (Abreu; Nascimento, 2018). With the growth in the number of devices connected to the internet, the digitization of essential services, and the growing reliance on digital data, cyber threats have become a critical risk to governments, businesses, and citizens.

Contemporary cyber threats are characterized by their complexity, global scale, and speed of propagation. Attacks such as ransomware, data leakage, and exploitation of unknown vulnerabilities have become increasingly frequent and sophisticated. In the view of Cavalcante and Lima (2021), there is a strong correlation between technological advancement and the increase in malicious activity, especially in strategic sectors such as health, finance, and critical infrastructure.

The main objective of this study is to analyze cybersecurity amid the increasing digitalization of human activities, with an emphasis on identifying risks, threats, and mitigation strategies in interconnected environments. To achieve this goal, the research proposes, at first, to examine the main current cyber threats, such as ransomware attacks and data breaches, mapping their origin, impact, and evolution. Next, it seeks to assess the vulnerability of critical infrastructures in the face of increased technological interdependence and the actions of organized criminal groups. Finally, the study aims to investigate the most effective information security practices and policies, taking into account emerging technologies, international regulations, and the strategic role of cybersecurity in geopolitical relations.

The motivation for this study lies in the increasing sophistication and danger of cyber threats in an increasingly digital and interconnected world landscape. Digital transformation, driven by technologies such as the Internet of Things (IoT), artificial intelligence (AI), and cloud computing, has exposed governments, businesses, and individuals to considerable risk. These risks compromise not only the integrity and confidentiality of data, but also the availability and continuity of services considered essential for the functioning of society.

The notorious increase in cyberattacks targeting critical infrastructure – such as hospitals, public transport systems, and power distribution networks – demonstrates the urgent need to implement more robust and effective digital protection strategies. Added to this is the growing professionalization of cybercrime, often associated with complex geopolitical interests, which elevates cybersecurity to the level of a global strategic issue.

In this context, it is essential to understand the fundamentals, the multifaceted challenges, and the possible solutions in the field of information security. Only in this way will it be possible to ensure the resilience of digital systems, protect sensitive information, and preserve social, economic, and political values in an era characterized by hyperconnectivity and increasing dependence on digital technologies. The research is justified, therefore, by its relevance for security and stability in the contemporary world.

2 METHODOLOGY

This study adopted a qualitative research approach, having as its main research strategy the literature review method. The choice of this methodology is justified by the need to obtain a comprehensive and in-depth understanding of the fundamental concepts, complex challenges, and significant advances related to cybersecurity in the context of accelerated digital transformation and increasing exposure to technological risks in all sectors of the economy and society.

The literature review allowed us to map the main contemporary cyber threats, which constantly evolve in terms of sophistication and impact, as well as to identify the most effective practices, policies and technologies that have been adopted by organizations of different sizes and segments to strengthen their resilience and responsiveness in the face of digital attacks.

To carry out the literature review, several sources of information were consulted, including academic reference works in the area, scientific articles published in specialized journals, institutional reports prepared by government agencies and security agencies, and detailed technical documents produced by consulting companies and technology suppliers.

The coverage period of the sources consulted was from 2018 to 2024, with the aim of capturing the most recent trends and the most relevant changes in the cybersecurity landscape. Priority was given to sources with recognized relevance and high credibility in the areas of information security, cybersecurity and digital governance, ensuring the quality and reliability of the data collected. Among the main theoretical frameworks used, authors such as Abreu and Nascimento (2018), who address the fundamentals of information security, Barbosa and Mattos (2021), who analyze the main cyber threats, Brandão and Reis (2019), who discuss strategies for preventing and detecting attacks, and Cavalcante and Lima (2021), who explore issues related to governance and management of information security, stand out.

Updated technical reports have also been incorporated, such as ENISA's Threat Landscape Report 2023 (2023), which offers a comprehensive overview of the threat landscape in Europe, and specific studies on digital security governance and culture (NUNES; ASSUMPTION; BRUSTOLIN, 2022; QUERINO; ARAÚJO, 2021), which highlight the importance of organizational and behavioral aspects in protecting against cyberattacks.

The survey, selection and critical analysis of the bibliographic material made it possible to understand the evolution of digital threats over the last few years, the impact of the COVID-19 pandemic on information security, which accelerated the digitization of various activities and increased exposure to risks, the growing professionalization of cybercrime, which has been organized into complex and profitable structures, and the most effective solutions for risk mitigation, such as the use of SIEM (Security Information and Event Management) tools, which allow the monitoring and analysis of security events in real time, the performance of SOCs (Security Operations Centers), which offer monitoring and incident response services 24 hours a day, and the implementation of internationally recognized security norms and standards, such as ISO/IEC 27001, which sets out the requirements for an information security management system. The review also contemplated the Brazilian legal context, especially with regard to the General

Data Protection Law (LGPD), whose guidelines directly influence the security policies adopted by organizations that collect and process personal data of Brazilian citizens.

The systematization and synthesis of the information obtained through the literature review allowed the construction of a critical and comprehensive analysis of the current situation of cybersecurity and the importance of integrated practices that consider not only the technical aspects of protection against attacks, but also the organizational, cultural and regulatory factors that influence the effectiveness of security measures. Thus, the methodology adopted proved to be adequate to the purpose of the study, offering a solid basis for the discussion and interpretation of the results obtained and for the formulation of practical recommendations for the improvement of cybersecurity in organizations.

3 RESULTS

This study reveals a worrying increase in the sophistication and incidence of cyberattacks in recent years, with essential sectors such as healthcare, energy, and public administration being preferred targets. The ENISA report (2023) points to a 25% increase in cyber threats compared to previous years, underscoring the pressing need for robust and effective defense strategies.

High-profile events, such as the attack on the Colonial Pipeline in the United States, which resulted in severe disruptions in fuel supply, serve as emblematic examples of the destructive potential of cyberattacks (Silva, 2023). This incident, which affected the supply of several American states, demonstrated the vulnerability of critical infrastructures and the ability of cybercriminals to cause significant disruption to the economy and society. Similarly, in Europe, several hospitals have been targeted by ransomware attacks, which have compromised their systems and disrupted patient care, putting lives at risk and highlighting the severity of the consequences that can come from cybersecurity failures.

The COVID-19 pandemic acted as a catalyst for the worsening of this scenario, accelerating the digitization of various activities and driving the intensive use of digital platforms, remote work, and the adoption of personal devices for professional purposes, often without the implementation of adequate security measures. This sudden and widespread change exposed a number of vulnerabilities that were promptly exploited by cybercriminals, as evidenced by several studies, such as that of Costa and Souza (2022), which analyzed the impact of the pandemic on cybersecurity.

In addition, the exponential growth of the phenomenon known as "shadow IT" – which refers to the use of applications, services and technological devices that are not authorized or managed by the organization's IT team – has contributed significantly to the expansion of the attack surface.

By using unsupervised tools and platforms, employees can inadvertently open security breaches and expose sensitive data to risks, making the task of protecting the company's digital assets even more complex.

Given this situation, it is imperative to rethink the approach to cybersecurity, prioritizing awareness and the adoption of safe practices by all employees, in addition to strengthening security infrastructures. Companies must invest in cutting-edge technologies and training in order to create a resilient workforce that is able to respond quickly to incidents, minimizing the impacts of future attacks.

A finding of great importance in this study lies in the observation of the progressive professionalization of cybercrime, which has manifested itself in an increasingly organized and sophisticated manner. Highly structured criminal groups, often with the veiled or explicit support of certain States, have started to operate with well-defined divisions of labor and complex business models, going so far as to offer "attacks-as-a-service", a practice that has become increasingly common and is known as Cybercrime-as-a-Service (Teixeira, 2020).

These groups use underground forums and hidden networks on the dark web to market malicious tools, share information about newly discovered vulnerabilities, and offer on-demand attack services, which makes carrying out cyberattacks accessible even to individuals with little technical knowledge but the financial resources to hire these services.

The analysis carried out also unequivocally demonstrated that effective digital protection transcends the mere implementation of isolated and punctual technological solutions. Cyber governance, to be truly effective, requires the implementation of structured and comprehensive information security policies, the establishment of well-defined and documented processes, and the adoption of international security standards and norms, such as ISO/IEC 27001, which establishes the requirements for an information security management system (ISMS).

The use of widely recognized frameworks, such as the NIST Cybersecurity Framework, can help organizations structure their cyber defenses in a systematic way and in line with the best practices in the market. In the Brazilian context, the General Data Protection Law (LGPD) plays a central role in regulating the processing of personal data, establishing clear rules and obligations for companies that collect, store, and use information from Brazilian citizens (Nunes; Assumption; Brustoln, 2022). Failure to comply with the LGPD can lead to severe sanctions, including high fines and restrictions on the operation of companies.

One of the crucial points that emerged from the survey was the finding that cultivating an organizational culture deeply rooted in digital security is a determining factor for the effective protection of a company's assets. This culture implies that all employees, regardless of their

hierarchical level or role, have a clear understanding of the cyber risks that the organization faces and feel personally responsible for actively contributing to the protection of the company's data, systems, and information.

In other words, digital security should be seen not only as a responsibility of the IT team, but as a core value that permeates the entire organization and influences the behavior of all its members.

The implementation of continuous and comprehensive training programs, which cover everything from the basics of information security to the most sophisticated threats, and the implementation of regular awareness campaigns, which use different communication channels and formats to disseminate information about security, are essential measures to mitigate risks such as phishing attacks, social engineering attempts, and the misuse of sensitive data (Querino; Araújo, 2021). Simulating cyber incidents, through hands-on exercises and realistic scenarios, has proven to be an effective tool to prepare teams to respond in a coordinated and efficient manner in crisis situations, minimizing damage and downtime.

Finally, the research highlighted the fundamental relevance of early detection of cyber threats, which can be achieved through the implementation of advanced technologies, such as SIEM (Security Information and Event Management), which allows the collection, analysis, and correlation of suspicious events and behaviors in real time. These SIEM tools are capable of identifying abnormal patterns and malicious activity that may indicate the occurrence of an attack in progress.

Combined with the performance of SOCs (Security Operations Centers), which operate 24 hours a day, 7 days a week, continuously monitoring the organization's network, systems, and applications, and reacting proactively to security incidents, this type of structure considerably increases the resilience of organizations in the face of digital threats (Santos; Pazinatto; Cunha, 2024). SOCs are made up of teams of cybersecurity experts who use monitoring and analysis tools to identify, investigate, and respond to security incidents, ensuring business continuity and the protection of the organization's data.

4 DISCUSSION

In recent years, there has been a worrying escalation in the number and sophistication of cyberattacks. According to ENISA's Annual Threat Report (2023), there has been a 25% increase in cyber threats compared to previous years, with sectors such as healthcare, energy, government, and critical infrastructure standing out. This increase is due, in part, to the increasing digitalization of processes and the greater interdependence of connected systems.

One of the most alarming aspects is the number of incidents involving critical infrastructure, such as hospitals, airports, power plants, and water supply networks. The attack on the Colonial Pipeline in the United States in 2021, for example, caused fuel shortages in several states and demonstrated the destructive potential of a successful cyber action (Silva, 2023). In Europe, hospitals have been targeted by ransomware, disrupting medical care and putting lives at risk.

The COVID-19 pandemic has acted as a catalyst for this increase in threats. The growth of remote work, the massive use of digital platforms, and the pressure for fast and accessible solutions have exposed security gaps in several organizations (Costa; Souza, 2022). The use of personal devices without adequate protection, vulnerable home networks, and the growth of *shadow IT* (unauthorized technologies within companies) have facilitated the action of cybercriminals.

Another relevant factor is the professionalization of cybercrime. Organized groups, often with state support, operate international attack networks, sell vulnerabilities on underground forums, and even offer *Cybercrime-as-a-Service* attacks, facilitating access to sophisticated tools even for individuals with little technical knowledge (Teixeira, 2020).

As the digital threat landscape becomes more intricate and persistent, the need for a strategic and comprehensive approach to cybersecurity intensifies. This approach must transcend the mere implementation of isolated technological tools, encompassing the smooth integration of robust governance practices, the cultivation of a conscious and proactive organizational culture, the implementation of continuous and vigilant monitoring, and the establishment of strict access controls.

Cybersecurity governance translates into the implementation of well-defined policies, optimized processes, and strict controls, with the primary objective of ensuring that organizations adequately protect their sensitive data and critical systems. Internationally recognized standards, such as ISO/IEC 27001, widely adopted frameworks, such as the NIST Cybersecurity Framework, and specific legislation, such as the General Data Protection Law (LGPD) in Brazil, play an essential role in this complex and multifaceted process (Nunes et. al., 2022).

The creation and strengthening of an organizational culture intrinsically focused on digital security represent one of the most effective factors to mitigate cyber risks. This entails the continuous and comprehensive training of all employees, from end users to specialized technical teams and management leaders, so that they are able to promptly recognize and respond appropriately to threats such as phishing, social engineering, and misuse of confidential information (Querino; Araújo, 2021).

The implementation of well-structured awareness programs, regular training, and the promotion of continuous educational campaigns are essential practices for the development of this safety culture (Santos et. al., 2024). Additionally, conducting realistic simulations of cyber incidents helps prepare employees for real crisis situations, transforming them into active agents engaged in the organization's cyber defense.

Early detection of cyber threats fundamentally depends on the ability of organizations to continuously monitor their digital assets, identifying suspicious activity and anomalous behavior in real time. The implementation of solutions such as SIEM (Security Information and Event Management) allows for the collection, correlation, and comprehensive analysis of security events, providing valuable insights into the state of the organization's security (Nunes et. al., 2022).

In addition, SOCs (*Security Operations Centers*) function as operations centers dedicated exclusively to cybersecurity, where teams of specialized professionals constantly monitor networks, investigate incidents in a timely manner, and coordinate effective responses 24 hours a day, 7 days a week (Querino; Araújo, 2021). The combined use of SIEM solutions and the operation of a SOC significantly increases the ability to react to cyber incidents, minimizing the time of exposure to threats and reducing the potential for damage.

5 CONCLUSION

The comprehensive analysis conducted in this study makes it clear that cybersecurity is not just a technical concern, but rather an urgent and pressing strategic need, given the increasing digitization of virtually all human activities and the ever-increasing complexity of threats permeating the digital environment. From an in-depth investigation of the main contemporary cyber risks, it became evident that sectors considered critical to the functioning of society – such as health, energy, government, and transport infrastructure – have become preferred targets for sophisticated, coordinated, and increasingly frequent attacks.

The survey also consistently demonstrated that while technological solutions play a key role in protecting against cyberattacks, effectiveness in digital defense depends on a multidimensional and integrated approach, which includes sound and transparent governance, well-structured and comprehensive information security policies, the adoption of international security norms and standards, such as ISO/IEC 27001, and strict adherence to current legislation, such as the General Data Protection Law (LGPD) in Brazil.

The growing professionalization of cybercrime, with emphasis on practices such as Cybercrime-as-a-Service, significantly expands the reach and impact of threats, making it essential to implement constant vigilance and early detection of security incidents.

Another crucial aspect pointed out by the survey was the urgent need to foster an organizational culture genuinely focused on information security, which involves the promotion of regular and personalized training for each area of the company, the realization of creative and impactful awareness campaigns, and the simulation of cyber incidents to test the readiness and responsiveness of the teams.

Building a workforce that is prepared, up-to-date, and aware of digital risks is as relevant as the implementation of advanced security tools, such as SIEM (Security Information and Event Management), and the performance of specialized security centers, such as SOCs (Security Operations Centers).

In conclusion, the research demonstrates that cyber resilience requires a strategic and balanced combination of cutting-edge technology, well-defined processes, and empowered and engaged people. In an increasingly connected, complex world exposed to cyber threats, only organizations that adopt a proactive, systemic, and integrated posture in relation to information security will be able to ensure the continuity of their operations, protect their sensitive information against unauthorized access, and preserve their reputation and the trust of their customers and partners in the face of the inevitable threats of the digital environment.

ACKNOWLEDGMENT

We thank God first for granting us wisdom, strength and perseverance throughout this journey. To our families, we express our deepest gratitude for the unconditional support, love, patience and encouragement, which have been essential for the accomplishment and completion of this work. We would also like to thank the Coordination for the Improvement of Higher Education Personnel (CAPES) for the financial support through the granting of a scholarship, which made the development of this research possible.

REFERENCES

Abreu, V., & Nascimento, L. (2018). Segurança da informação: Um estudo sobre a tríade CIA nas organizações. Revista Científica de TI, 5(2), 22–31. Recuperado de https://www.fatecsp.br/dti/tcc/tcc0023.pdf

Aguiar, T. H. (2021). Políticas de segurança cibernética no Brasil: De onde viemos e para onde vamos. LACNIC. Recuperado de https://www.lacnic.net/innovaportal/file/6974/1/politicas-de-seguranca-cibernetica-no-brasil-de-onde-viemos-e-para-onde-vamos-thais-helena-aguiar-pt.pdf

Barbosa, F., & Mattos, E. (2021). Integridade da informação em ambientes críticos: Análise e soluções. Revista de Sistemas de Informação, 17(1), 55–68. Recuperado de https://www.egape.pe.gov.br/images/media/1665420043_Apostila%20Introducao%20Seguranca%20Informacao%20Corporativa.pdf

Brandão, V., & Reis, C. (2019). A importância da segurança da informação no contexto corporativo. Revista de Administração e Inovação Digital, 4(1), 100–114. Recuperado de https://codebit.com.br/blog/seguranca-da-informacao/importancia-seguranca-da-informacao-empresas

Cavalcante, J., & Lima, P. (2021). Ransomware e infraestruturas críticas: O caso do STJ. Segurança Cibernética em Foco, 2(4), 18–29. Recuperado de https://cdn-amm.diariomunicipal.org/publicacoes/2019/11/25/6196_1e156988…pdf

Costa, M., & Souza, B. (2022). Continuidade de negócios e disponibilidade da informação. Revista Brasileira de Segurança Digital, 9(3), 77–89.

European Union Agency for Cybersecurity. (2023). Threat Landscape Report 2023. Recuperado de https://www.enisa.europa.eu

Nunes, I. A., Assunção, J. Z. de, & Brustolin, V. (2022). Análise estrutural das estratégias de segurança cibernética do Brasil e dos Estados Unidos. Revista Brasileira de Estudos de Defesa, 9(2), 227–250. https://doi.org/10.26792/RBED.v9n2.2022.75246

Querino, L. de F., & Araújo, R. G. M. de. (2021). A resiliência cibernética? Conscientização de micro e pequenas empresas. In Digital 5 – E-book. Recuperado de https://ci.fdc.org.br/AcervoDigital/E-books/2021/Digital%205/Digital%205%20-%20cap%206.pdf

Santos, J. M., Pazinatto, F. A. C., & Cunha, L. E. C. (2024). Desafios na gestão da segurança cibernética: O papel estratégico do gestor de tecnologia na era da computação em nuvem. RECIMA21, 5(10). https://doi.org/10.47820/recima21.v5i10.5665

Silva, J. P. da. (2023). Inteligência artificial aplicada à segurança da informação. São Paulo: Atlas. Recuperado de https://revistas.unipam.edu.br/index.php/perquirere/article/view/2040

Teixeira, M. (2020). Riscos cibernéticos em infraestruturas críticas. Revista Segurança Digital, 10(1), 80–99. Recuperado de https://muniosecurity.com/ataques-ciberneticos-em-infraestruturas-criticas-aumento-de-30/