ISSN 1816-6075 (Print), 1818-0523 (Online)
Journal of System and Management Sciences
Vol. 13 (2023) No. 4, pp.574-582
DOI:10.33168/JSMS.2023.0434

Evaluation of Cyber Sabotage in Public Entities

Francisco Hilario, Milner Liendo, Laura Chipana, Renee Rivera

Universidad César Vallejo, Carretera Panamericana Norte Km 695, Los Olivos, Lima, Perú

fhilariof@ucvvirtual.edu.pe, mdavilareba@ucvvirtual.edu.pe, lachipanaro@ucvvirtual.edu.pe, rriveracr@ucvvirtual.edu.pe

Abstract. The purpose of this study is to carry out an evaluation of cyber sabotage in public entities based on the state policies that govern within an infrastructure in the field of cybersecurity, through reviews of research and scientific articles. In addition, this research was conducted in order to help technologists expand their knowledge about the tools, method and effectiveness of being able to employ metrics to mitigate multiple anomalies within entities. On the other hand, the study method was with a qualitative approach, based on a methodology of scientific research with case study methods, to achieve the objective of analyzing the strategic situation outlining the policies of public entities, discuss supported issues and considerations later raised by the subject. Therefore, the expected results tend to summarize the basic structure of these strategies, including the priorities and main problems identified in relation to the countries studied, to determine the general model of the strategy, taking into account the political background of the countries, and to propose future development by comparing the current situation. and the basic structure of these countries. Finally, if a cyberattack is successful, security recommendations will be provided, thus forming the basis for the protection of telecommunications networks and systems, allowing more people to become aware of lesser-known vulnerabilities in such systems.

Keywords: Cybersecurity, public entities, public policy, cyber sabotage.

1. Introduction

Currently, entities around the world have constant attacks by cyberspace, with harmful tools to corrupt data. They are seen at public events such as presidential elections, stealing information from banking institutions or hacking into government agency websites, each time in a different way. The number of users surfing the internet has increased exponentially, due to the proliferation of mobile devices, smart sensors and internet technologies, driven by the lockdowns imposed to mitigate the Covid-19 pandemic; The Internet is becoming a fundamental process of the daily lives and actions of people around the world.

According to Ghaleb et al. (2022) mentions most companies moved to the internet due to the availability of reliable infrastructure such as the cloud, cost-effective platforms and a large target market. However, the internet has many cyber threats such as malware, spam, phishing, financial fraud, information theft and data sabotage. Malicious websites are the main attack vector for cybercriminals to spread malware and malicious files. Based on Quiroga (2021) he stated that companies experience changes, such as their organization, new requirements, security and privacy standards, etc. The more the level of personnel in an organization the more essential the changes and privileged information of each user, each of these products carries with it a series of risks associated with results ranging from the most innocuous to the most disastrous, that is because companies try to try to maximize resilience. and to be able to absorb them without eloquently altering their organizational characteristics and thus be able to return to their original state once the disturbance has passed.

The use of ICT-enabled online platforms has become more common, allowing e-commerce to grow further during the pandemic, but carries security risks, such that Flores (2023) states that countries are increasingly reliant on online computing systems, but no tool in the internet world can take for granted that governments and organizations are doing their best to Minimizing the consequences and costs of inaction for proper network security management can be much greater. Therefore, over time, the topic of cyber security and information protection becomes very difficult, and more and more people hear about online hacks and cyber attacks against organizations' own systems, leading to the realization that this is the organization's most valuable asset. more important as we realize that there is our own capacity for information.

Regarding Baque (2021) he mentioned that network vulnerabilities consist of three components: computer, communication and power system. Attacks can simultaneously attack multiple systems and subsystems in specific remote locations, making them more interdependent. The safety level then indicates the severity of the damage that can be caused in the event of a power system breakdown. Over the years, cybersecurity has gone global. Computer security is especially focused on protecting the computer infrastructure, so it is the ability to identify and mitigate vulnerabilities related to computer problems.

Modern cybersecurity systems are inherently static and cannot make decisions or learn from events. Therefore, it is proposed to propose an intelligent technique suitable for IoT cybersecurity infrastructures, which can: subscribe to intrusion detection standards to prevent and respond to threats; Because threats change daily, making systems outdated and vulnerable. Therefore, teaching methods have been studied with the arrival of IoT technology to integrate them into a system that allows intelligent learning with unsupervised algorithms integrated into the selection method, thus achieving optimal results. The technological changes focused on the protection of information and contemplate the security in the vulnerabilities of different external organizations, it is essential to improve the development of these platforms for the social and economic progress of tools and telecommunications (Coello, 2021).

Finally, it is necessary to specify the importance of cybersecurity and the challenges faced by public entities. As it is known that information systems, cyberspace and cloud services are the basis for the administration and execution of personal and organizational data, it is necessary to protect privileged

information with services that can control the data encryption of each process or transfer of information. In the public management services, software is maintained that safeguards the data of each gradual process of the multiple projects or data of private interest, in the same way, it is necessary to consider that there are trained personnel complying with measures to mitigate anomalies that the data puts in evidence. Therefore, it is of great importance to take into account cybersecurity as the main issue for the information technology service because cybercriminals massively corrupt their goal of corrupting data, so it is important the specialized group to provide support to these problems, technological tools (high impact software), backup services, Cloud storage and encrypting data to take preventive measures. To conclude, the general problem was: How does the fundamentals of cybersecurity influence cyber sabotage in public entities?

2. Literary Review

The relevant theories shown in the research are presented below, segmenting ideas about cyber sabotage through cybersecurity, computer crimes and the management of ICT for the benefit of academic training.

2.1. Computer Crime

In the theory of Computer crime of Cross (2022) He explains that these are criminal groups that have gained more recognition for their legitimacy, but remain popular around the world because they are difficult to prevent or regulate, as cybercriminals have different protection options. nameless. Therefore, any act of using the software for electronic money transfers, telecommunications or password cracking will result in a fine of 3 to 6 years free or a fine of several days. (Lunarejo and Rodriguez, 2021).

2.2. Classification of Cybercrime

Since advances in ICT lead to the emergence of new illegal activities and their use to regulate existing illegal activities, an effort is made to categorize these activities into:

2.2.1. Pure cyberattacks

Pure cyberattacks for Cano (2020) states that there are all those newly created crimes that can be committed solely through the use of information technology as a means to perform specific actions that do not represent the category of the physical world, without affecting its ability to perform a specific behavior. conduct in traditional crimes. Meanwhile, Miró (2012) states that cyberspace and ICTs are facilitating the introduction of new goods and services of economic and social value and triggering new behaviors that can only be carried out through the use of ICTs. In this sense, a series of illicit activities characterized by damaging services, terminals or goods that operate in cyberspace. These are called pure cybercrimes because they only occur in cyberspace.

2.2.2. Replica cyberattacks

Cyberattacks replicated according to Miró (2012) are those actions that must not only be carried out in the physical world, but can also be carried out with the help of ICT through cyberspace. These behaviors are copies of cybercriminals when carrying out traditional crimes through the network, in this case the attack is carried out through the Internet, which is a new means of communication; However, due to the scale of criminal activities, many new acts arise.

2.3. Cybercriminal Profile

The cybercriminal according to Cámara (2020), must have specific skills and knowledge in the field of IT systems administration, which is characterized by the following: has IT knowledge or assumes strategic positions in the places where he works, handles confidential information or has access to systems and there are people, not in a strategic position, who can be active people because of their skills and knowledge in the field of information technologies, and therefore criminals in this regard. For Lunarejo and Rodríguez (2021) they affirm that cybercriminals are not common criminals, but IT

experts who have skills to manage and operate computer systems, work by trade in strategic locations and work with confidential information.

2.3.1. Hackers

For Cámara (2020) indicated that these are people who tend to violate the so-called inviolable procedures and systems for pleasure or other interests, enjoy exploring everything around them to understand how computer systems work. They are people who use this activity as an intellectual challenge for the sole purpose of deciphering and understanding computer systems without causing damage, manipulation, fraud, espionage or sabotage, but they are not allowed for entertainment purposes only.

2.3.2. Crackers

Fernández et al. (2019) points out that they are those people who access systems remotely with the intention of destroying data, denying service to users and causing problems in the computer system, processor or network, these people are the so-called electronic hackers; pirates use ready-to-use programs that they can buy online or create themselves; while hackers create their own software with knowledge of computer programs. Similarly, Belcic (2020), states that hackers create and crackers destroy in the sense that hackers aim to cause harm, such as stealing data by impersonating someone else or even using paid free software.

2.4. The Peruvian State in the face of cybercrime

The Peruvian state, faced with the advancement of technology and its enormous impact on crime, recognized the need to create standards to punish this new type of acts committed with the help of IT, so the legislator of 1991 of the Criminal Code as an innovative and pioneering position of new criminal ways; then, in 2000, with Law No. 27309, the first computer crime was included in the Criminal Code, so the legislator suggested modifying and aggravating some of the crimes typified in the current criminal regulations, adapting them to ICTs. However, these provisions do not correspond to the true nature of computer-related crimes, so the legislator considers it necessary to enact legislation that includes the parameters established by the Budapest Convention, giving rise to Law No. 30096, amended by Law No. 30171 due to the deficient and ambiguous nature of the former; In this sense, each normative step of Peruvian law related to current legislation on computer crimes must be known in detail.

3. Method

In this evaluation we have the analytical descriptive research, focused on the qualitative study, that is why we have the main attacks and vulnerabilities that have had a high environment worldwide in recent years, that is why the attacks have suffered important incidents; and targeted attacks through hacker groups, such as retaliation for political decisions of the central government. Likewise, the purpose of this study was to evaluate cyber sabotage in public institutions and what would be the strategies and solutions to mitigate these types of attacks on information and communications systems. For this, it is based on scientific research supporting the fundamental criteria of different previous theoretical studies that will provide the necessary help through journals and articles that will be fundamental for the support of the information of the research project, focus on a qualitative study, due to the use of many sources of information we will provide on how we can evaluate and mitigate cyber sabotage in public entities.

4. Results and discussion

Cybersecurity is key to ensuring the integrity of processes, allowing a digital environment to thrive in the administrative processes of government organizations. Several topics were discussed.

- Detail and evaluate the fundamentals of cybersecurity.

- Innovation of legal, normative methods.
- Policy creation.

It is critical to develop and use cybersecurity standards to mitigate threats and prevent cyberattacks. Benefit the confidentiality, availability and integrity of information.

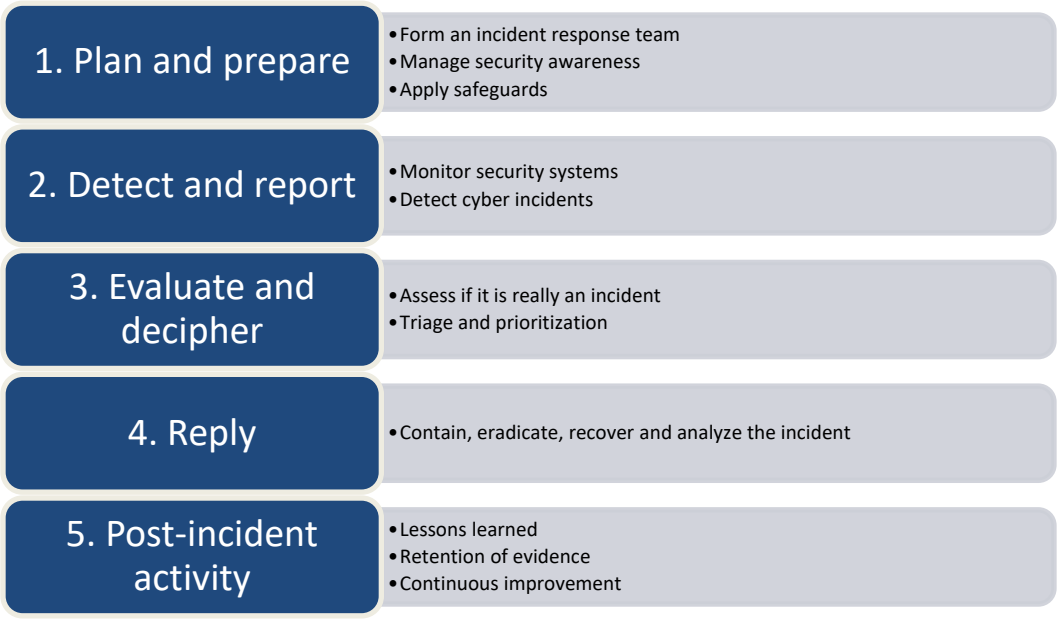

Fig. 1: Key elements for cybersecurity

In addition, thanks to the ability to deploy various types of anti-attack tools, all of them will be improved to prevent future attacks.

Fig. 2: Current state of biosecurity 2021

Source: *Analysis of cyberattacks on public organizations in Ecuador and their administrative impacts (Coello, 2021)*

Cybersecurity models were determined through systematic searches in bibliographic references and the internet. The following were determined:

- Model ISM3
- Perimeter security model
- Clark-Wilson Model
- Thin Security Model
- Bell-LaPadula Model
- Zero Trust Model
- Defense-in-depth model

Once the models were defined, they were reduced to a more reasonable number, taking into account

the opinions of the authors of academic scientific articles on cybersecurity; for which a matrix of priorities was developed.

Table 1: Prioritization matrix

	Relationship to the research topic	Integrity	Availability	Confidentiality	Total
ISM3	1	2	2	1	6
Perimeter Security	4	3	3	2	2
Clark-Wilson	2	4	2	1	9
Thin-Security	5	4	4	3	16
Bell-LaPadula	2	2	3	4	11
Zero Trust	5	4	4	5	18
Defense in Depth	4	4	3	4	15

In a business where data information can be processed, emergency projects are a necessary service. According to Leiva (2021), no business continuity plan, public or private, also has a cyber incident response plan, and there are few alternatives before a disaster (natural or provoked). The impact of the threat will help us determine the countermeasures that the organization or company should choose.

It can be affirmed that the results obtained are consistent with the work of Salinas (2022), who promoted the development of a proposal that takes into account the specificity and detail of the cybersecurity plans and projects of the first countries in the world, such as the United States, Russia and China have supported him to develop a proposal for a cybersecurity organization model in Spain. The study is also based on a comparative analysis of the necessary cybersecurity models deployed in public organizations of these characteristics for the preparation of applications. In addition, his research is qualitative and descriptive.

For their part, Gómez et al. (2022) in their research work Centralization of computer security system analysis with Alienvault Ossim, it is practical for network administrators to use security data collectors for network management and monitoring, and favors awareness and understanding. Use tools that make it easy to optimize anomaly detection and resolve various network issues. It is open source and costs zero. This study is consistent with the use of the cybersecurity model as a tool to protect information on online platforms. The study is also qualitative and descriptive; which offers an example of application of the proposed tool so that you can discover its usefulness and functionality.

Likewise, Veramendi, (2021) has evaluated the threat detection systems: Snort and Suricata, analyzing the effectiveness of attacks that act as a criterion to compare both tools; Like our research, the results allow a simulation of real toxic flow in the tests of the websites, gaining knowledge about the operation of the invasion systems, especially Snort and Suricata, detailed investigations. Although his research was a quantitative approach, and the development of the research project did not have much similarity with what was explained in this scientific article; We agree that security is not only based on the comparison of network security models or tools, but also on detailed contingency or softening case plans to avoid abnormalities and guarantee security data.

5. Conclusion

In conclusion, security is a concept that helps organizations protect their privileged information in the face of continuous technological changes and advances in the development of new tools, and cybersecurity is a strategic balance between interrelated areas that require guiding principles, premises and priorities.

Similarly, public facilities that have a major impact on data security will conceptualize different designs to prevent different attacks targeting public and private facilities. Taking into account the various changes in vulnerabilities in cyber and cyberspace, different technological frameworks are implemented to protect and deal with anomalies with warnings, take the necessary measures against the various attacks that can damage information and ensure the security of the information tunnel with the organization itself taking care of the organization. It also limits overall system performance due to the need to train anomaly detectors. Training data may or may not reflect the actual system network model, which can lead to performance degradation. Improvements to the current system, including improvements to previous restrictions, are left for future work.

Therefore, proposals for cybersecurity models can be developed with a new approach for government organizations in the era of digital transformation, taking into account characteristics such as integrity, security and availability. Multifactor authentication, protection of external endpoints, integration of security solutions to the cybersecurity architecture, analysis of changes of common users and differentiated pyramid risk management structure with levels of strategic, operational and tactical control.

Acknowledgements

We are very grateful to all the people who contributed knowledge and made this article a success.

References

Baque, R. (2021). Design of a workstation for vulnerability detection of web servers, to mitigate cyberattacks [Southern State University of Manabí]. http://repositorio.unesum.edu.ec/bitstream/53000/3186/1/BAQUE%20VILLEGAS%20ROBERTH%20ANDR%C3%89S.pdf

Chamber, S. (2020). Cybercriminology and the profile of the cybercriminal. *Law and Social Change*, 60, 470–512. https://dialnet.unirioja.es/servlet/articulo?codigo=7524987

Cano, Q. (2020). Phenomenology of cybercrime. https://cibercrim.com/fenomenologia-de-la-ciberdelincuencia/

Chango, R., & Gualpa, D. (2023). Implementation of ethical hacking tests to evaluate the computer security system in the company Rhelec Ingeniería CIA. LTDA [Salesian Polytechnic University]. https://dspace.ups.edu.ec/bitstream/123456789/24450/1/TTS1228.pdf

Coello, I. (2021). Analysis of cyberattacks in public organizations in Ecuador and their administrative impacts [Salesian Polytechnic University]. http://dspace.ups.edu.ec/handle/123456789/20738

Cruz, J. (2022). E-commerce and its impact on computer crimes, La Libertad, 2021 [César Vallejo University]. https://repositorio.ucv.edu.pe/handle/20.500.12692/97317

Fernández, J. C., Miralles, F., & Millana, L. (2019). Psychosociological profile in the cybercriminal. *RICSH Ibero-American Journal of Social and Humanistic Sciences*, 8(16), 156–177. https://doi.org/10.23913/ricsh.v8i16.179

Chango, R., & Gualpa, D. (2023). Implementation of ethical hacking tests to evaluate the computer security system in the company Rhelec Ingeniería CIA. LTDA [Salesian Polytechnic University]. https://dspace.ups.edu.ec/bitstream/123456789/24450/1/TTS1228.pdf

Gayoso, V., Hernandez, L., & Arroyo, D. (2020). Cybersecurity. CSIC. https://www.digitaliapublishing.com/a/80863

Ghaleb, F. A., Alsaedi, M., Saeed, F., Ahmad, J., & Alasli, M. (2022). Cyber Threat Intelligence-Based Malicious URL Detection Model Using Ensemble Learning. *Sensors*, 22(9), 3373. https://doi.org/10.3390/s22093373

Gómez, E., Bermeo, O., & Arévalo, L. (2022). Analysis of centralized computer security systems through the Alienvault Ossim tool. *Ecuadorian Science Journal*, 6(1), 23-31. https://doi.org/10.46480/esj.6.1.181

Gorjón, M. (2021). Computer sabotage to critical infrastructures: Analysis of the criminal reality contained in articles 264 and 264 bis of the penal code. Special reference to its commission for terrorist purposes. *Journal of Criminal Law and Criminology*, 25. https://doi.org/10.5944/rdpc.25.2021.28405

Kurniawan, Y., & Mulyawan, A. (2023). The role of external auditors in improving cybersecurity of the companies through internal control in financial reporting. Journal of System and Management Sciences, 13(1), 485–510. https://doi.org/10.33168/JSMS.2023.0126

Leyva, A. (2021). Analysis of cybersecurity public policies. Study of the Ecuadorian case. Pole of Knowledge: *Scientific - Professional Review*, 6(3), 1229-1250.

Lunarejo, E., & Rodriguez, K. (2021). The lifting of the secrecy of communications in computer crimes [César Vallejo University]. https://repositorio.ucv.edu.pe/handle/20.500.12692/76869

Marin, L. (2023). Cybersecurity and its impact on teleworking in a public entity, Lima 2022 [César Vallejo University]. https://repositorio.ucv.edu.pe/handle/20.500.12692/106398

Medina, P. R., & Cando, M. R. (2021). Prevention in cybersecurity: focused on technological infrastructure processes. *3C ICT*, 10(1), 17–40. https://doi.org/10.17993/3ctic.2021.101.17-41

Ordoñez, S., Márceles, K., & Amador, S. (2022). An adaptable Intelligence Algorithm to a Cybersecurity Framework for IIOT. *Engineering and Competitiveness*, 24(2), 1–13. https://doi.org/10.25100/iyc.v24i2.11762

Pérez, E. (2023). Corporate governance and cybersecurity: Some challenges for the administrative body. *Journal of Company Law*, 67, 2. https://dialnet.unirioja.es/servlet/articulo?codigo=8849864

Pérez, M. (2022). Quantitative evaluation of cybersecurity technological risks in a digital transfer application in a Peruvian financial institution, period 2021-2022 [Universidad Inca Garcilaso de la Vega]. http://repositorio.uigv.edu.pe/handle/20.500.11818/6919

Quiroga, S. (2021). Design of the information security management system—ISMS in Aerocivil for the Information Technology Management process (GINF 6.0). [National Open And Distance University –

UNAD]. https://repository.unad.edu.co/handle/10596/41282

Roldan, M. T., & Vargas, H. F. (2020). Cybersecurity in mobile telecommunications networks and their risk management. *Engineering and Development*, 38(2), 279-297. https://www.proquest.com/scholarly-journals/ciberseguridad-en-las-redes-móviles-de/docview/2484005928/se-2

Salinas, A. (2022). Cybersecurity Model for Municipal Savings Banks in Times of Digital Transformation—A New Approach [Universidad Privada del Norte]. https://repositorio.upn.edu.pe/handle/11537/29733

Serna, T., & Gonzales, A. (2022). The "Autonomous" SOC: Artificial intelligence for the new cybersecurity. *Journal of Information Units*, 19. https://ruidera.uclm.es/xmlui/bitstream/handle/10578/30871/EL%20SOC%20AUTONOMO.pdf?sequence=1&isAllowed=y

Urbanovics, A., & Guajardo, R. (2022). Cybersecurity strategies in Latin American countries – a comparative analysis. [Cybersecurity Strategies in Latin American Countries – a Comparative Analysis] *Acta Hispanica, Suppl.IV*, , 89-104. https://doi.org/10.14232/actahisp.2022.0.89-104

Veramendi, A. (2021). Evaluation of threat detection systems: Snort and Suricata [University of the Basque Country]. https://addi.ehu.es/handle/10810/53353.

Zambrano, A. (2021). The use of mobile banking in computer crimes against heritage in the city of Arequipa, 2020 [César Vallejo University]. https://repositorio.ucv.edu.pe/handle/20.500.12692/62306