Advanced Research on Information Systems Security

ISSN: 2795-4609 | ISSN: 2795-4560
Print & Online

Predicting Cybersecurity Risk - A Methodology for Assessments

Daniel Ferreira[a,b]*, Henrique São Mamede[c]

[a]*Universidade de Trás-os-Montes e Alto Douro, Vila Real, Portugal*
[b]*LAPI2S - Laboratory of Privacy and Information Systems Security & COPELABS, Porto, Portugal*
[c]*Universidade Aberta, Lisbon, Portugal*
[a]*Email: danielferreirapessoal@gmail.com*
[c]*Email: hsmamede@gmail.com*

Abstract

With the current impulse of Cyberattacks, data becomes of central importance. Many challenges in how they are used also have to be discussed.
Defining a suitable cybersecurity incident response model is a critical challenge that all companies face today. A high number of incidents happen daily and for which there is not always an adequate response. This is due to the lack of data-based predictive models (evidence). There is a significant investment in research to identify the main factors that can cause such incidents, always trying to have the most appropriate answer and ultimately boosting responsiveness and success. At the same time, several different methodologies assess organizations' risk management and maturity level.

Keywords: risk; cybersecurity; information; nist; iso

* Corresponding author. Email: danielferreirapessoal@gmail.com

1. Introduction

The current post-COVID-19 context has accelerated uncertainties regarding the issue of Cybersecurity and the Risks associated with it. Most organizations were not prepared for the decision to start operating remotely, also coexisting with the local operation, creating a hybrid model, which created new vulnerabilities for organizations

[32]. The transformation that they had to carry out on themselves to remain operational in the market brought to light a whole issue regarding Cybersecurity and Security that until then was half asleep, as it was an issue that most companies looked at as a cost and without a benefit or a return on investment that could be considered measurable.

The dichotomy between approaching risk and the inability to respond to security incidents is addressed in the book "Risk Assessment and Decision Analysis with Bayesian Networks" [1] in which it is stated "that popular methods such as risk registers and heat maps are insufficient to adequately deal with risk assessment". On the other hand, the book "Visualization Analysis" [2] refers to the "clear advantages of using data visualization to understand better the connections between these data compared to using textual or numerical forms". It is known that data visualization plays a vital role in the decision-making process, which helps build a narrative regarding decision-making based on information, and how that decision can be the right one.

With access to this knowledge, managers who work in Cybersecurity can make decisions quickly, when necessary, evaluate investment and return, and the criticality of their decision, with visualization and interpretation being considered critical skills for those managers [3].

While other researchers have investigated trends within current definitions and uses of risk in Cybersecurity, few have come up with formalized definitions of cybersecurity risk. For example, Oltramari and Kott [4] suggest that practitioners describe cyber risk in terms of a system's configuration rather than the likelihood of damage occurring. They also investigated the process of identifying specific risks for various systems. A study on risks to supervisory control and data acquisition (SCADA) systems defined risk management as "coordinated activities to direct and control an organization about risk" and risk assessment as the "general process of identifying risk, risk analysis, and risk assessment" [5].

As well as a more visual analysis of data, companies can become more competitive and achieve more success using data analysis and visualization [6], [7], as they can react more quickly to any potential situation. The visualization and use of data thus come to help in the decision-making process that is fundamental for any organization, no matter the size or nature and can influence all the components of the system [8], the quality of information is vital and necessary for effective decision making [9].

2. Theoretical background and preliminary literature review

As previously described, management is quite comprehensive, and the panoply of existing Standards and Frameworks cannot always give a concise answer without the need to interconnect two or more Frameworks.

These are based on controls to be implemented, which sometimes do not give us the desired visibility through indicators, which can be correlated so that organizations can make the right decisions in a preventive way. An example is the compilation by ENISA [35] (ENISA, European Union Agency for Ciber Security) of the number of Tools and Frameworks related to Risk Management in Security and Cybersecurity, as described below. Enisa [35] has identified a collection of well-known and widely used RM - Risk Management-related frameworks and methodologies that provide high-level guidelines for risk management processes that can be applied across all

types of organizations, as mentioned in the compilation. As illustrated in the following Figure, it is intended to collect the necessary theoretical basis, dividing it into five blocks regarding the research:

1. NIST Cybersecurity Framework: Most used framework reference that compiles controls from other frameworks.
2. ENISA Cybersecurity Framework: Framework based on other frameworks and intended to provide a European vision.
3. ISO27005 Risk for Information Security: Reference of the ISO Standard in the scope of Risk Management in Security.
4. RMF - Risk Management Framework: Framework designed by ISACA that aims to provide a comprehensive view of risk management in various domains.
5. Review of Existing Frameworks: What research and documentation exist in this area and maturity assessments that respond to the challenge addressed.

3. Cybersecurity Risk Analysis

Currently, research carried out on the IEEE Xplore Portal points out that the future may gain consistency in Serverless "solutions" promising to be faster, better and more robust.

In terms of security, serverless architectures help to improve the level of security or at least make it easier, contributing to this the excellent advantage of Serverless being mainly focused on the code and not on the servers that run it. Vendors manage all aspects of configuring servers for the customer [46].

However, although these architectures contribute to increased security, not everything is as it seems, as for example some attack scenarios have already been explored using weak permissions in Amazon AWS to escalate privileges [47]. The research explains how an attacker who exploits a weak policy can retrieve credentials or create permanent access to the target account [48].

Thus, from here we infer that although the architectures that are beginning to be designed to be more secure in the services they provide, they have their challenges in terms of security. Risk analysis is a process that must precede any evaluation of an organization regarding services and architectures, it is also, and must be, a process of learning and proactivity of an organization when it intends to anticipate any change in the way it operates the its services, thus preventing any incident that may happen, or minimizing the risks of this potential incident, for this it is essential to have indicators of analysis and trends, to anticipate, predict and minimize the risk of this potential incident, reacting proactively.

3.1. Framing of risk analysis in Cybersecurity

Risk analysis is transversal to all sectors of society, in the document defined by the Cybersecurity Information Sharing Act of 2015, which authorizes and encourages private companies to take defensive measures to protect and mitigate cyber threats, as well as the sharing of information regarding indicators of cyber threats. [10].

3.2. The way of communicating and interpreting

One of the biggest challenges is in risk communication. Although there are standards and guidelines, each organization makes its assessment and interpretation of these same risks, often in an inconsistent way because the data does not exist, being done empirically, which leads to deviations associated with biases that are aggravated by the lack of standardization [11]. The importance of standardized terminology was demonstrated across disciplines and in interdisciplinary work. For example, the lack of standardized vocabulary contributed to the reduction of innovation in research studies because they could not be used as a comparison with other research works due to differences in terms used [12]. Vocabulary standardization is commonly established by creating a formalized and systematic nomenclature that facilitates communication between stakeholders from various disciplines [13] [34]. To facilitate cybersecurity communication, Ramirez recommends that practitioners initiate change using technical language compatible across disciplines. They also argue that a standardized cybersecurity vocabulary starts with increasing research efforts focused on identifying trends in terminology standards [14]. Ramirez further suggests four sub-disciplines of Cybersecurity: public policy, computer science, management, and social science [15].

3.3. Use of data, visualization, and interpretation

One of the significant challenges is the interpretation of data, its use, and interpretation as a way of responding in advance to a potential event. When analyzing and discussing risks, those responsible for risk management focus on the CIA pillars (Confidentiality, Integrity, and Availability) as the only risk indicators [16], [35]. Others suggest that a holistic model of cybersecurity risk incorporates variables other than the CIA, precisely time and people, as crucial factors in assessing risk to a system, network, or user [17]. An example of this risk assessment and its impact on different pillars is that the image below is very expressive. It uses a statistical analysis that allows the visualization of the data and its trend.

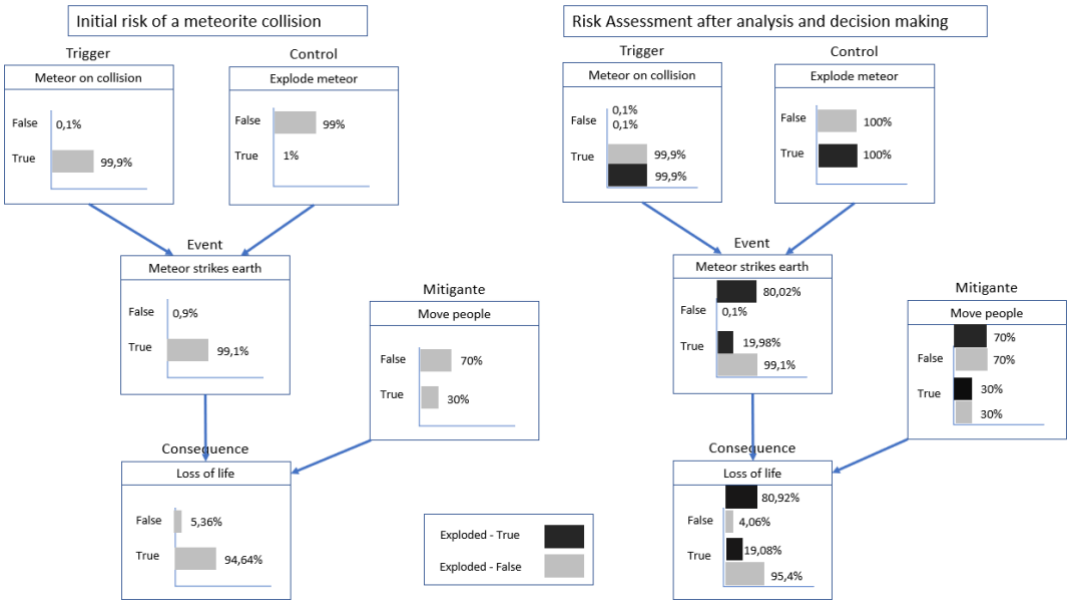

Figure 1 - Risk Analysis based on data

Looking at the values for the probability of "Loss of Life" being false, we found that we jumped from just over 4% (when we do not react) to 81% (when we react). This massive increase in the chance of saving the world clearly explains why it was worth a try.

The main benefits of this approach are:

- Risk measurement is more meaningful in context, in stark contrast to the simple "risk = probability x impact" approach, where none of the concepts has an unambiguous interpretation.
- Uncertainty is quantified, and we can read the current probability values associated with any event at any stage.
- Provides a visual and formal mechanism for recording and testing subjective probabilities. This is especially important for an event with little or no relevant data.

4. Risk management in cybersecurity and success factors

A recent 2021 study on cybersecurity trends found that 68% of business leaders believe their cybersecurity risks are increasing [28], [37]. On the other hand, implementing organizational cybersecurity involves installing security software. On the contrary, it is also a complex undertaking that involves multifaceted technological, organizational, and process issues [2], [38]. Despite the vibrant security market and the multidimensional complexities surrounding cybersecurity, a comprehensive cybersecurity Critical Success Factors framework to guide cybersecurity management in organizations still needs to be developed. While some review articles in the literature on cybersecurity success factors [3], [39] focus on issues such as cybersecurity policy, processes, and procedures, for critical infrastructures and information security factors based on existing Frameworks for decision-making, [37] summarize 12 factors that influence security decisions: vulnerability, compliance and policy, risk, physical security, continuity, infrastructure, confidentiality, integrity, and availability (CIA), security management, awareness, resources, and access control, and factors organizational.

4.1. Existing frameworks reviewed and analyzed

In the reviewed literature sources and mainly in the compilation carried out by ENISA [35], [40], it was possible to identify several Risk Management frameworks and standards adapted for security and Cybersecurity.

The table below presents an overview of these frameworks, their use, and the review carried out by third parties. However, each covers its focus from the perspective of risk management, and none of them explicitly identifies which indicators should be taken into account for a data-based approach that translates into indicators that can be used proactively. In this work developed by ENISA [35], [41] and other researchers, we understand the need to create a more focused methodology on management indicators and data that can be used proactively.

Table 1 - Reviewed Maturity & Readiness Models – ENISA[35]

Framework Model	Author

ISO/IEC 27005:2018 'Information technology — Security techniques — Information security risk management	ISO/IEC
NIST SP 800-37 Rev. 2 is an asset-based RMF	NIST
NIST SP 800–30 REV.1 Guide for Conducting Risk Assessments	NIST
NIST SP 800–82 REV. 2 Guide to industrial control systems (ISC) security	NIST
The OCTAVE Method (Operationally Critical Threat, Asset, and Vulnerability Evaluation)	Carnegie Mellon University / Software Engineering Institute - USA
ISACA RISK IT FRAMEWORK	ISACA
INFORMATION RISK ASSESSMENT METHODOLOGY 2	Information Security Forum
ETSI TS 102 165-1, THREAT VULNERABILITY AND RISK ANALYSIS (TVRA)	ETSI Technical Committee Cyber Security
MONARC	Cyber Security Agency, Luxemburg
EBIOS RISK MANAGER	ANSSI, France
MAGERIT V.3: ANALYSIS AND RISK MANAGEMENT FOR INFORMATION SYSTEMS	Spanish Ministry for Public Administrations
EU ITSRM, IT SECURITY RISK MANAGEMENT METHODOLOGY V1.2	EU, DG DIGIT
ENTERPRISE RISK MANAGEMENT – INTEGRATED FRAMEWORK	COSO - Committee of Sponsoring Organizations of the Treadway Commission, USA

By analyzing the broad collection of RM frameworks and methodologies presented in the previous table, we identified several factors that limit the potential of RM frameworks and methodologies. These include the following:

- Use of quantitative or qualitative (or semi-quantitative) methods for risk assessment;
- Use of specific, extensible, or reusable catalogues or libraries (e.g. to support asset assessment, identification of risks or vulnerabilities, selection of security controls, etc.);
- Risk calculation method (e.g., most methodologies use one of the formulas risk = Impact x Probability, Risk = Impact x Threat Probability x Vulnerability Level, or similar formula);

The interoperability potential of different frameworks and methodologies is related to the identified features. For example, if performing a risk assessment following a methodology relies on a specific catalogue of threats or vulnerabilities, the methodology's ability to adopt an alternative catalogue in the context of an interoperable framework will be limited.

Overall, extensive review and analysis of a large set of RM frameworks and methodologies allowed us to identify many features that can be used as a basis for designing and implementing an interoperable cybersecurity RM

framework with a robust posture.

5. Problem Identification and Research Question(s)

Cybersecurity risk management has been applied to many aspects of modern life, including banking, finance, healthcare, life, business ventures and project management [4].

Despite several existing works on cybersecurity risk management, the literature does not present works considering such contextual information when performing risk management for critical infrastructures [12], [41].

[8] Elucidates the growing number of cyberattacks that require Cybersecurity and forensic experts to detect, analyze, and defend against cyber threats in near real-time.

It turns out that both the organization nor the vendors do not have a complete understanding of what information is considered CTI (Cyber Threat Intelligence), so more research is needed to define CTI [1].

Cyber Threat Intelligence (CTI) provides evidence-based information to prevent threats. Existing works and industry practices emphasize the need for CTI and provide methods for threat intelligence and sharing. However, despite these significant efforts, there is a lack of focus on how CTI information can support CSRM activities so that the organization can proactively carry out appropriate controls to mitigate risk.

These attacks are now more sophisticated, multi-vector and less predictable, making the Cybersecurity Risk Management (CSRM) task more challenging [18], [42].

Through analysis to obtain more reliable and realistic solutions, level of understanding, quality of Doctoral Thesis Project knowledge, level of cybersecurity and threats uncertainty, and sensitivity levels of model parameters are integrated into the model parameters to analyze Cybersecurity and threats [13], [43].

Having in consideration the reviewed literature, we have then summarized our two research Problems:

RP1: While some assessment models are developed to assess the extent to which the organization can manage cybersecurity risks, there is a gap in existing models to assess the readiness of organizations to successfully achieve and maximize the expected results of effective risk management in Cybersecurity.

RP2: Organizations face a significant threat from new attack vectors while lacking the resources and strategy to compete with new business models. To maximize the results related to effective cybersecurity risk management, organizations need support with action plans to mitigate their readiness gaps (lay the groundwork), mature the organization, to respond effectively and securely, maximizing the return on the investment.

Our research questions can then be summarized:

- RQ1: Does the Visualization of risk-related data facilitate the decision-making process?
- This RQ1 focuses on the identified problem 1 (RP1)
- RQ2: Could the Visualization of Risk Information be an asset in the investment decision and help to clarify the ROI in security?

- This RQ2 focuses on the identified problem 2 (RFP2)

6. Conceptual Model - Methodology for Predictive Cyber Security Risk Assessment (PCSRA)

Currently, the existing risk management models are based on existing standards and frameworks, always with a view to responding to the controls that these standards describe. Whenever a risk assessment is carried out, it is based on the response to these controls, if they exist, if they are implemented, and what are the opportunities for improvement.

Nowadays, people are already talking about predictive risk management models, but these predictive models continue to be based on the same form of risk analysis, since when we talk about Cybersecurity, we are talking about a part that comprises the organization's infrastructure, its networks, the web, and much more, everything that circulates in the famous Cyberspace. Therefore, Risk Management must proactively change the way it is approached, and it is on this new approach to responding to Risk that the model presented is based.

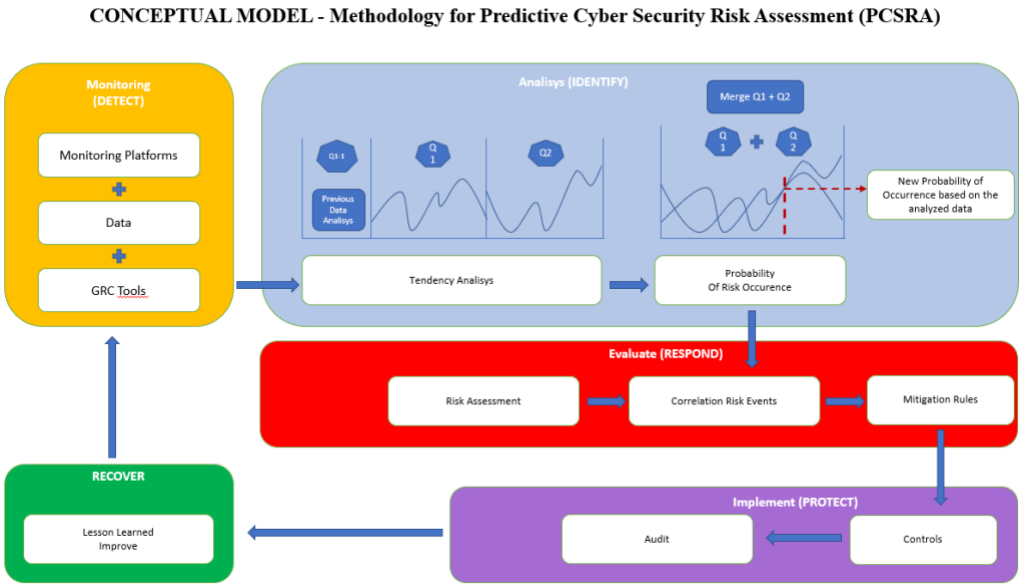

Figure 2 - Conceptual Model for PCSRA

How does the presented model differ?

Let's see, currently, organizations have monitoring tools such as SIEMs, Vulnerability Management, among others, that allow them to have access to data, data that, when properly processed, are valuable information in a risk analysis based on trends, now the model presented is that's right, to present a model that correlates the existing and applied controls, with this data analysis, the tendency of a certain risk to happen again.

The present model intends to have an approach that meets other existing ones, and intends to integrate them, adding value in the identification and Management of Risk.

- **Monitoring (DETECTED)**

- This phase intends to use the currently existing tools as a way of detecting possible and possible risks existing in the organization, through monitoring platforms and GRC - Platforms dedicated to the controls applied in organizations and their relationship with the compliance.
- Here we can detect all possible risks either passively or actively.

- **Analysis (IDENTIFY)**
  - At this stage, it is possible, through an analysis, as in the example, to understand which trends are derived from the monitoring platforms, and by overlaying the analysis of trends, to make a prediction that such a risk will occur again, thus preparing the organization for a more assertive answer based on the data it already has, leading it to give a more consistent answer, as well as with more real costs of the measures that must be adopted.
- **Evaluate (RESPOND)**
  - At this stage, the answer is intended to be given with mitigation measures based on the assessment of the existing risk and on the correlation of events originated by the platforms, because by reconciling these 2 factors we will be able to have more effective and efficient mitigation responses, which will be the target of application of more effective controls, irrespective of their nature.
- **Implement (PROTECT)**
  - This is the phase of implementing the controls and measures necessary to mitigate the risks and minimize the exposure factor of the organization to risks of any nature. After the implementation of controls and measures, they must be Audited to ensure that everything is in accordance with the stipulated.
- **RECOVER**
  - This is the recovery phase after the risks have already been dealt with. Here, an analysis of continuous improvement and lessons learned will be carried out, that is, it is a phase to make an assessment of the existing needs for improvement, where it will be possible for us to be affected again and why, where we should focus our risk management, and what learning we withdraw for the future.

Ultimately, the model presented must be executed whenever a new risk analysis is carried out in the organization. It should be used as an effective check when performing a cybersecurity risk analysis. It is not intended to only assess risk management based on controls, but in a more comprehensive and transversal way, but rather to assess how embedded the culture and mentality is in the way the organization manages risk, and how well structured it is, is the organization for risk appetite, prioritizing the right initiatives and tracking the measures to be implemented. Organizations, irrespective of their size, will have the ability to continually assess the risk management component and will be able to act in resolving these same risks.

7. Research Strategy

This research will apply the Design Science Research (DSR) methodology to develop a user-friendly model that supports all companies to assess their fundamentals regarding Cybersecurity, considering it from the organization's perspective, aiming to support the resolution of the research identified problems (1 and 2).

We selected DSR because it is a problem-solving approach with a clear objective to enhance human knowledge, develop innovative artifacts, and solve problems through them [14], [44], [45].

Considering our identified research problems, questions and objectives, the target is to develop an artifact to support the resolution of the identified problems, answer the research questions and achieve the research objectives. The DSR is an accepted research methodology in this field to support developing and evaluating innovative artifacts.

Within the DSR, we selected the model proposed by Peffers [23], a widely consensual design science methodology [23]. The main reason for this selection is related to its simplicity. Although more focused on theoretical review in the transition from objective to design than Hevner's approach [14], it fits better with current research, especially since readiness is not a well-defined tangible asset to investigate in the organization’s environment. At the same time, it provides a practical, highly problem-oriented and objective solution-oriented process, guiding us from problem identification (and its relevance) to the design and development of a possible solution, its demonstration and communication.

This research method will provide a well-defined framework for navigating problem identification to developing and evaluating a solution. Using the DSR Peffers model (as illustrated in Figure 4), we will design and develop a model that will be tested in selected companies. The output of this test will be accessed and communicated within the scientific community.

The model (Methodology for Predictive Cyber Security Risk Assessment (PCSRA) two components can be summarized as follows:

1. Assess if the visualization of risk-related data facilitates the decision-making process - A proposed initial assessment will be done via the shortest possible questionnaire written in simple language that any employee should understand. The results of this questionnaire will be computed, and a readiness state will be calculated, considering how the senior leaders rated the different pillars. The gap between employees and senior leaders will impact the end-readiness state
2. Clarified RoSI in Security - the assessment’s output will lead to identifying the risk levels incurred in the calculated readiness state and identify possible actions to be taken as a step to move the company to a

higher readiness state. Those actions will be presented to the company in a document that describes what is needed to execute those actions, close the gaps & mitigate the risks.

8. Conclusion

We selected DSR because it is a problem-solving approach with a clear objective of improving human knowledge, developing innovative artifacts and solving problems through them [14], [44], with the objective of supporting the resolution of the problems the research identified problems (1 and 2).

Within the DSR, we selected the model proposed by Peffers [23], a widely consensual design science methodology [23]. The main reason for this selection is related to its simplicity. Although more focused on the theoretical review on the transition from purpose to design than Hevner's approach [14], it fits better with current research, especially as readiness is not a well-defined tangible good to investigate in the organization's environment. At the same time, it provides a practical, highly problem-oriented and objective solution-oriented process, guiding us from problem identification (and its relevance) to the conception and development of a possible solution, its demonstration and communication.

The model (Methodology for Predictive Cybersecurity Risk Assessment (PCSRA) two components can be summarized as follows:

1. Evaluate whether the visualization of risk-related data facilitates the decision-making process;
2. Security-enlightened RoSI - the outcome of the assessment will lead to the identification of risk levels incurred at the calculated state of readiness and the identification of possible actions to be taken as a step towards moving the enterprise to a higher state of readiness.

9. Future work

After the elaboration and complete validation of the PCSRA, future research works can be done in the integration of this model with the processes of risk management in the organizations.
This risk management must be perfectly in tune with the governance model and the objectives of the organization [39].
For this, it will be useful to deepen the research in integration with:

1. Frameworks to proactively manage the implementation of risk analysis according to existing standards.
2. Frameworks to efficiently continue risk management and that allow the integration of the PCSRA as a model to be used and of reference for proactive risk management, after the implementation of the PCSRA, answering the questions: is it possible to predict a new risk and in that way were to prevent

potential impacts on the organization? If so, what structure can be used to lead and manage this risk management program? [12].

3. Frameworks for designing the risk management strategy and making an RBS [11].
4. Finally, a scorecard should be developed to give visibility to the information being produced, in order to measure the success of the PCSRA implementation.

10. Final considerations

This paper presents a literature review regarding the decision-making process using Information Visualization. With a detailed analysis, it was possible to assess that of the resources studied and researched, few refer to this type of decision-making based on risk analysis and using visualization tools as the main results of the author's work. The research shows that there is some degree of research in the field of Information Visualization to support decision-making, but not in the field of security risk analysis, we could not identify very deep research in this field, and no significant research (as mentioned only two) in the field of InfoVis to support organizations in decision making. With organizations facing challenges in this area, the potential for faster decision-making through Information Visualization can be of great support and value, helping increase the organization's valuation and ability to proactively respond to the most challenging security risk.

References

[1] Abu MS et al (2018) Cyber threat intelligence–issue and challenges. Indones J Electr Eng Comput Sci 10(1):371–379

[2] Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How the integration of cyber security management and incident response enables organizational learning.

[3] Atkins, S., & Lawson, C. (2020). An Improvised Patchwork: Success and Failure in Cybersecurity Policy for Critical Infrastructure.

[4] Balla Moussa Dioubate & Wan Daud, Wan Norhayate, A Review of Cybersecurity Risk Management Framework in Malaysia Higher Education Institutions, 10 May 2022

[5] Bowen, B. M., Devarajan, R., & Stolfo, S. (2011). Measuring the human factor of cyber security. Paper presented at 2011 IEEE International Conference on Technologiesvfor Homeland Security (HST), Boston, MA. (230–235). IEEE;

[6] Chad Ashley, Michelle Preiksaitis, Strategic Cybersecurity Risk Management Practices for Information in Small and Medium Enterprises, ARTICLES Published 2022-06-01

[7] Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., & Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. Computers & Security, 56, 1–27;

[8] Conti M, Dargahi T, Dehghantanha A (2018) Cyber threat intelligence: challenges and opportunities. Cyber threat intelligence. Springer, Berlin, pp 1–6

[9] Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. Technology Innovation Management Review, 4(10), 13–21;

[10] Cybersecurity Information Sharing Act of 2015;

[11] Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. Computers and Security, 92(2020), 1–21

[12] Halima Ibrahim Kure, Shareeful Islam & Haralambos Mouratidis, An integrated cyber security risk management framework and risk predication for the critical infrastructure protection, Neural Computing and Applications (2022)

[13] Hakan AKYILDIZ, A Conceptual Model of Port Cybersecurity and Threats: Knowledge and Understanding, Year 2022, Volume, Issue 21, 23 - 32, 18.05.2022

[14] Hevner, A.R., March, S.T., Park, J., & Ram, S. (2004). Design Science in Information Systems. MIS Quarterly, 28(1), 75-105.

[15] Hussain, A., Mohamed, A., & Razali, S. (2020). A review on Cybersecurity: Challenges & emerging threats. NISS 2020 Proceedings, 1–7. Marrakech, MR: ACM

[16] ISO27005 Information security risk management;

[17] ISO31000 Risk Management.

[18] Kure, H. and Islam, S. 2019. Cyber Threat Intelligence for Improving Cybersecurity and Risk Management in Critical Infrastructure. Journal of Universal Computer Science. 25 (11), pp. 1478-1502

[19] Manoj, B., & Baker, A. (2007). Communication challenges in emergency response. Communications of the ACM, 50(3), 51–53;

[20] NIST 800-53 Risk Management Framework;

[21] NIST Cybersecurity Framework

[22] Oltramari, A., & Kott, A. (2018). Towards a reconceptualizationreconceptualization of cyber risk: An empirical and ontological study. Journal of Information Warfare, 17(1);

[23] Peffers K, Tuunanen T, Rothenberger A, and Chatterjee S. (2007) "A design science research methodology for information systems research," Journal of Management Information Systems

[24] Ramirez, R., & Choucri, N. (2016). Improving interdisciplinary communication with standardized cyber security terminology: A literature review. IEEE Access, 4, 2216–2243;

[25] Ramirez, R. B. (2017). Making cyber security interdisciplinary: Recommendations for a novel curriculum and terminology harmonization (Thesis, Massachusetts Institute of

[26] Risk Assessment and Decision Analysis with Bayesian Networks;

[27] RMF -Risk Management Framework;

[28] Sobers, R. (2021). 134 Cybersecurity Statistics and Trends for 2021. https://www.varonis.com/blog/cybersecurity-statistics/

[29] S. Lohr, "The age of big data", New York Times, vol. 11, 2012;

[30] S.K. Card, J.D. Mackinlay, and B. Shneiderman, "Readings in information visualization: using vision to think", In Morgan Kaufmann, 1999;

[31] T. Munzner, "Visualization analysis", 2014;

[32] Yeoh, W., Huang, H., Lee, W. S., Al Jafari, F., & Mansson, R. (2021). Simulated phishing attack and embedded training campaign.

[33] Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102;

[34] W. Eigner, "Current Work Practice and Users' Perspectives on Visualization and Interactivity in Business Intelligence.", 17th International Conference on Information Visualization, 2013;

[35] https://www.enisa.europa.eu/publications/compendium-of-risk-management-frameworks

[36] Mario Saraiva, Nuno Mateus-Coelho, CyberSoc Framework a Systematic Review of the State-of-Art, Procedia Computer Science, Volume 204, 2022, Pages 961-972, https://doi.org/10.1016/j.procs.2022.08.117.

[37] William Yeoh , Shan Wang , Ales Popovic , Noman H. Chowdhury, A Systematic Synthesis of Critical Success Factors for Cybersecurity, 2022, https://doi.org/10.1016/j.cose.2022.102724

[38] N. Mateus-Coelho and M. Cruz-Cunha, "Serverless Service Architectures and Security Minimals," 2022 10th International Symposium on Digital Forensics and Security (ISDFS), 2022, pp. 1-6, doi: 10.1109/ISDFS55398.2022.9800779.

[39] Sultan AlGhamdi, Win Khin Than Elena Vlahu-Gjorgievska, Information security governance challenges and critical success factors: Systematic review, 2020, https://doi.org/10.1016/j.cose.2020.102030

[40] M. Saraiva and N. Coelho, "CyberSoc Implementation Plan," 2022 10th International Symposium on Digital Forensics and Security (ISDFS), 2022, pp. 1-6, doi: 10.1109/ISDFS55398.2022.9800819.

[41] Cuchta, Tom & Blackwood, Brian & Devine, Thomas & Niichel, Robert & Daniels, Kristina & Lutjens, Caleb & Maibach, Sydney & Stephenson, Ryan. (2019). Human Risk Factors in Cybersecurity. 87-92. 10.1145/3349266.3351407.

[42] M.M. Cruz-Cunha, N.R. Mateus-Coelho (Eds.), Handbook of Research on Cyber Crime and Information Privacy, IGI Global (2021)

[43] Alnatheer, Mohammed. (2015). Information Security Culture Critical Success Factors. Proceedings - 12th International Conference on Information Technology: New Generations, ITNG 2015. 731-735. 10.1109/ITNG.2015.124.

[44] F. Alves, N. Mateus-Coelho and M. Cruz-Cunha, "ChevroCrypto – Security & Cryptography Broker," 2022 10th International Symposium on Digital Forensics and Security (ISDFS), 2022, pp. 1-5, doi: 10.1109/ISDFS55398.2022.9800797.

[45] Duarte, N., Coelho, N., Guarda, T. (2021). Social Engineering: The Art of Attacks. In: Guarda, T., Portela, F., Santos, M.F. (eds) Advanced Research in Technologies, Information, Innovation and Sustainability. ARTIIS 2021. Communications in Computer and Information Science, vol 1485. Springer, Cham. https://doi.org/10.1007/978-3-030-90241-4_36.

[46] Nuno Mateus-Coelho; Manuela Cruz-Cunha, Serverless Service Architectures and Security Minimals, https://ieeexplore.ieee.org/abstract/document/9800779

[47] A. Lopez et al., "A cloud-based framework for machine learning workloads and applications", *IEEE Access*, vol. 8, pp. 18681-18692, 2020.

[48] T. Asghar, S. Rasool, M. Iqbal, Z. U. Qayyum, A. N. Mian and G. Ubakanma, "Feasibility of Serverless Cloud Services for Disaster Management Information Systems", *Proceedings - 20th International Conference on High-Performance Computing and Communications 16th International Conference on Smart City and 4th International Conference on Data Science and Systems HPCC/SmartCity/DSS 2018*, pp. 1054-1057, 2019.