Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 219 (2023) 1555–1563

Procedia Computer Science

www.elsevier.com/locate/procedia

CENTERIS – International Conference on ENTERprise Information Systems / ProjMAN – International Conference on Project MANagement / HCist – International Conference on Health and Social Care Information Systems and Technologies 2022

# Methodology for Predictive Cyber Security Risk Assessment (PCSRA)

Daniel Jorge Ferreira[a,d], Nuno Mateus-Coelho[b,d], Henrique S. Mamede[c]

[a]*Universidade de Trás os Montes e Alto Douro, Vila Real, Portugal*
[b]*IPCA – Polytechnic Institute of Cavado and Ave, Barcelos, Portugal*
[c]*INESC TEC, Universidade Aberta, Lisbon, Portugal*
[d]*LAPIS2S – Laboratory of Privacy and Information Systems Security, Porto, Portugal*

**Abstract**

With the current impulse of Cyberattacks, data becomes of central importance. There are many challenges in how they are used that also need to be discussed. Defining the suitable cybersecurity incident response model is a critical challenge that all companies face today. With a high number of incidents that happen daily and for which there is not always an adequate response due to the lack of predictive models based on data (evidence), there is a significant investment in research to identify the main factors that can cause such incidents, in and consistently trying to have the most appropriate answer, and ultimately, boosting responsiveness and success. At the same time, there are several different methodologies to assess the risk management of organizations and their level of maturity. The capability assessment is intended to enable organizations to understand better the fundamentals that need to be laid down to deliver cybersecurity successfully. There is, however, a gap in determining an organization's degree of proactive responsiveness to successfully embracing cybersecurity and an even more significant gap in assessing it from a risk management perspective. This work proposes a model to assess this capacity.


Peer-review under responsibility of the scientific committee of the CENTERIS – International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies 2022

*Keywords:* Risk, Cybersecurity, Data, Information Visualization, NIST, ISO, RMF

* Corresponding author.
E-mail address: danielferreirapessoal@gmail.com


Peer-review under responsibility of the scientific committee of the CENTERIS – International Conference on ENTERprise Information Systems / ProjMAN - International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies 2022
10.1016/j.procs.2023.01.447

## 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, only some 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 of 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 are vital and necessary for effective decision making [9].

## 2. Cybersecurity Risk Analysis

Risk analysis is a process that precedes any assessment of an organization. It is also an organization's learning and proactive process when it wants to predict any incident. For this, it is essential to have analysis indicators to anticipate and predict this incident and proactively react.

### *2.1. Framing of risk analysis in Cybersecurity*

Risk analysis is transversal to all sectors of society, as we can see in the image of fig. 1, illustrated by the Cybersecurity Information Sharing Act of 2015 which authorizes and encourages private companies to take defensive measures to protect and mitigate cyber threats. [10].

### *2.2. 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]. Ramirez recommends that practitioners initiate change using technical language compatible across disciplines to facilitate cybersecurity communication. They also argue that a standardized cybersecurity vocabulary starts with increasing research efforts focused on identifying trends in terminology standards [14]. Ramirez further suggests that cybersecurity has four sub-disciplines: public policy, computer science, management, and social science [15].

### *2.3. 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]. Others suggest that a holistic model of cybersecurity risk incorporates variables other than the CIA, specifically 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 expressive. The image below uses a statistical analysis to visualise the data and its trend.

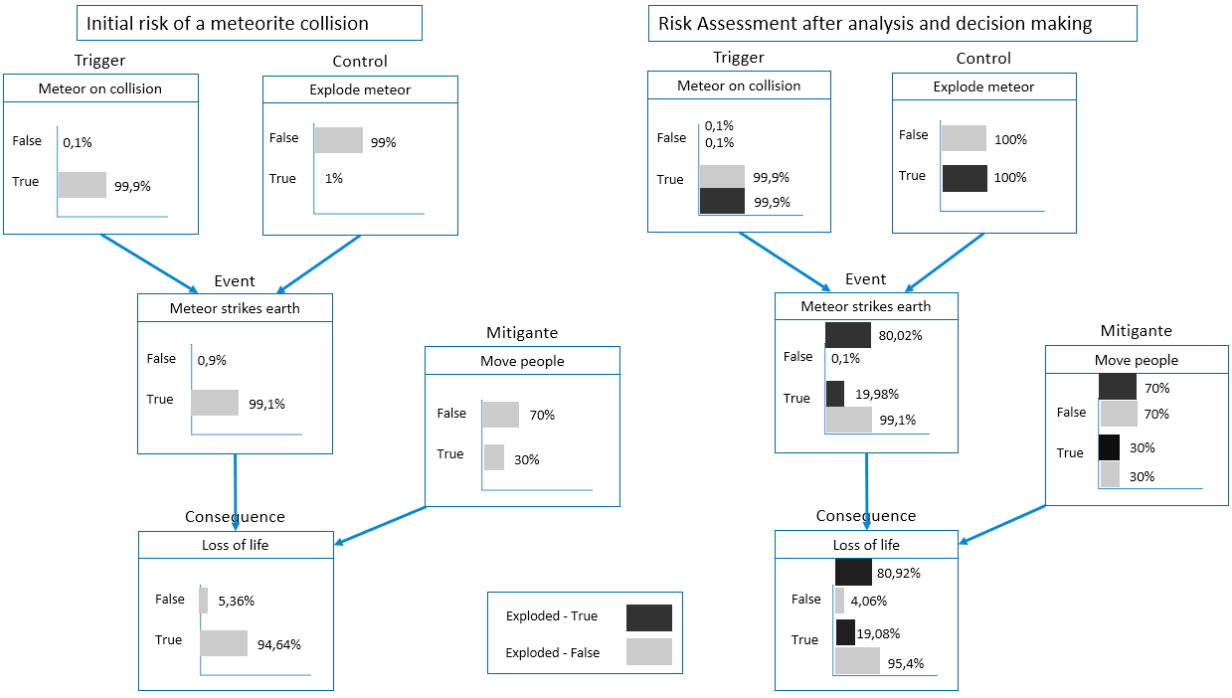


*Figure 1 - Risk Analysis based on data*

Looking at the values for the probability of "Loss of Life" being false, we found that we jumped from just over 4% (when we don't 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, this is in stark contrast to the simple "risk = probability x impact" approach, where none of the concepts has an unambiguous interpretation.
- Uncertainty is quantified and at any stage, we can simply read the current probability values associated with any event.
- Provides a visual and formal mechanism for recording and testing subjective probabilities. This is especially important for an event where we don't have much or no relevant data.

## 3. 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]. On the other hand, implementing organizational cybersecurity does not only involve installing security software, on the contrary, it is also a complex undertaking that involves multifaceted technological, organizational, and process issues [2].

Despite the vibrant security market and the multidimensional complexities surrounding cybersecurity, a comprehensive cybersecurity Critical Success Factors framework to guide cybersecurity management in organizations is still lacking. While there are some review articles in the literature on cybersecurity success factors [3], these focus on issues such as cybersecurity policy, processes, and procedures. for critical infrastructures, and information security factors based on existing Frameworks for decision making. Thus, what is verified is that in the existing literature this work is not guided by the theoretical component, which results in the lack of results-oriented toward the objectives oriented according to the Critical Success Factors for the methodology used in cyber security [39].

Assessing the success or failure of cybersecurity is a central topic when evaluating information systems (IS). Some studies approach the subject from a specific perspective, such as information security governance [43], culture [42], and human risk [41]; some focus on a specific IT artifact such as cloud computing [44], industrial control systems and critical infrastructure, others, however, use a holistic approach to investigating cybersecurity measures. For example, through a literature review and interviews with 19 experts, [44] 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 [40].

### *3.1. Existing frameworks reviewed and analyzed*

It was possible to identify several Risk Management frameworks and standards adapted for security and cybersecurity in the reviewed literature sources and mainly in the compilation carried out by ENISA [35], [38].

Table 1 presents an overview of these frameworks and their use, as well as the review carried out by third parties, however, each of them covers its focus from the perspective of risk management, and none of them specifically 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] and other researchers, we understand the need to create a more focused methodology on management indicators and data that can be used proactively.

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 catalogs or libraries (eg to support asset assessment, identification of risks or vulnerabilities, selection of security controls, etc.);
- Risk calculation method (eg 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 features identified above. For example, if performing a risk assessment following a methodology relies on a specific catalog of threats or vulnerabilities, the methodology's ability to adopt an alternative catalog 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.

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.

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 |

## 4. 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].

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

It turns out that both the organization and the vendors do not completely understand what information is considered CTI (Cyber Threat Intelligence), so more research is needed to define CTI [1], [37].

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 carry out appropriate controls to proactively mitigate risk.

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

Through analysis to obtain more reliable and realistic solutions, level of understanding, quality of 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],[36].

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 are facing 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. of the investment.

Our research questions can then be summarized in:

- 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)

## 5. Model Design

### *5.1. Design Science Research*

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 these artifacts [14].

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 the development and evaluation of innovative artifacts.

Table 2 illustrates the instantiation of the Peffers approach in our research work, detailing what will happen in each of the phases in more detail.

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

- **Does the Visualization of risk-related data facilitate the decision-making process** - A proposed initial assessment will be done via the shortest possible questionnaire written in a simple language that any employee should be able to understand. The results of this questionnaire will be computed, and a readiness state calculated, considering how the senior leaders rated the different pillars. The gap between employees and senior leaders will impact the end readiness state
- **Clarified ROI 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 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.

## 6. Final considerations

This methodology presents a literature review that reference refers to existing documentation regarding the decision-making process using Information Visualization using tools such as InfoVis.

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 profound 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 to increase the organization's valuation and ability to respond to the most challenging security risk. Proactively.

*Table 2 - Peffers framework instantiated to this research work (Peffers 2007)*

| Activity | Description |
|---|---|
| 1. ProblemsIdentification & and motivation | 1) Understand whether a model is possible to assess whether visualizing risk-related data facilitates an organization's decision-making process;<br>2) If so, how can that model enable a small or medium enterprise to improve the success of their implementation is based on a fix the foundations' plan |
| 2. Define the objectives for a solution | A model will be proposed for all organizations |
| 3. Design & Implement | The title of the designed model is **"Methodology for Predictive Cyber Security Risk Assessment (PCSRA)"**<br>The goal is that the model will<br>1. Does the Visualization of risk-related data facilitate the decision-making process<br>2. Propose and trigger a "**clarified ROI in Security"**, a component that identifies the risks at each state and possible actions that can be taken to move to the next state<br>The model will provide a document explaining the different readiness states, the basis behind the different categories in each state and actions that might be taken to mitigate the identified gaps. |
| 4. Demonstration | This model will be applied in organizations that are implementing cybersecurity risk management or intend to start. Five or more companies will be invited to use this model as part of their Cybersecurity Risk Management process. The model will be applied in organizations with more than 50 employees, and preferably covering several sectors. |
| 5. Evaluation | The success of PCSRA will be measured through a questionnaire with a "closed" answer format. The answers will be on a scale of 1 to 10, to be answered by business senior leaders.<br>While measuring the results, a target of success will be defined on a scale of 1 to 10:<br>• **Result = 1**: "The model did not provide valuable information, or the suggested actions did not positively impact the organization".<br>• **Result = 5**: "The model did provide valuable information, but the results wereachieved partially. It has proven to be helpful."<br>• **Result = 10**: "The model did provide valuable information, and enabled a set of decisions that converted to more successful outcomes out of the cybersecurity journey" |
| 6. Communication | The work will be communicated to the scientific community through the publication of different papers. |

## 7. Final considerations

This methodology presents a literature review that reference refers to existing documentation regarding the decision-making process using Information Visualization using tools such as InfoVis.

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 profound 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 to increase the organization's valuation and ability to respond to the most challenging security risk. Proactively.

## 8. Future Work

After the PCSRA has been fully developed and validated, future research work can be carried out integrating this model with cybersecurity risk management processes.

1. It will be useful for further research in integration with:
2. Frameworks to manage the implementation of cybersecurity risk management in any type of organization.
3. Frameworks for efficiently continuing an organization's cybersecurity risk management after the PCSRA is implemented, providing answers to the questions: Is cybersecurity risk management possible for any type of organization? If so, what can the organization do to lead and manage this cybersecurity program?
4. Frameworks for designing cybersecurity strategy through risk management.

Lastly, a scorecard can be developed to further improve the way of measuring PCSRA implementation success.

## 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);

[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,;

[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] 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.

[38] 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.

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

[40] 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.

[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] 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.

[43] 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

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