Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 219 (2023) 312–318

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

Cyber Resilience, a Survey of Case Studies

João Pavão[a], Rute Bastardo[b], Dário Carreira[c], Nelson Pacheco Rocha[d,*]

[a]*INESC-TEC, Science and Technology School, University of Trás-os-Montes and Alto Douro, Vila Real, Portugal.*
[b]*UNIDCOM, Science and Technology School, University of Trás-os-Montes and Alto Dou-ro, Vila Real, Portugal.*
[c]*Instituto Universitário da Maia, Maia, Portugal, Portugal.*
[d]*IEETA, Department of Medical Sciences, University of Aveiro, Aveiro, Portugal.*

Abstract

Considering the potential magnitude and impact of cyber-attacks, organizations must be able to understand their capabilities to prevent, respond and re-cover from these attacks as well to implement and refine adequate resilience plans. Due to the importance of cyber resilience, this survey aimed to review relevant case studies published in the scientific literature. The identified case studies followed different approaches since some of them were focused on risk assessment and risk management processes and the complexity of their implementation, while others were focused on the use of well-known frameworks to assess cyber resilience or on proposing new cyber resilience frameworks and tools.

Keywords: Cyber resilience; Risk assessment; Risk management; Survey.

* Corresponding author. Tel.: +351234247292.
E-mail address: npr@ua.pt

10.1016/j.procs.2023.01.295

1. Introduction

More than 60% of the world's population is now online [1]. Approximately one million people join the internet each day, while more than two-thirds of humanity own a mobile device. What is known as the Fourth Industrial Revolution (4IR) is already bringing tremendous economic and societal benefits and the Internet of Things (IoT) can even help to lower CO_2 emissions by optimizing energy consumption and reducing traffic congestion [2-4].

All this growth constitutes a macro-level phenomenon with people and organizations more networked with each other, but which can be breached and affected in unexpected and malicious ways and presents “cascade failure” risks [5]. Successful attacks might not only impact the organizations, but also have systemic effects causing harm to the economy as a whole and even to the national security. The essence of the problem is about how to make or support critical decisions, where there is a lot of uncertainty and a potentially excessive cost of making mistakes. In other words, it is about risky decisions.

Certainly, given the current circumstances, the organizations seek for robust solutions and overall guidance for risk management. In this respect, based on wide professional input, standards and frameworks were developed for implementing and evaluating cyber resilience: the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) Information Security Management (ISO/IEC 27001), the National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST-CSF), the Cybersecurity Capability Maturity Model (C2M2) from the Department of Energy of the United States, the Information Security Forum (ISF), the Computer Emergency Readiness Team-Resilience Management Model (CERT-RMM) of Carnegie Mellon University, the Control Objectives for Information and Related Technologies (COBIT), and the Open Web Application Security Project (OWASP), among others [6].

This article aims to review the recent scientific literature to assess how cyber resilience has been implemented and how the above-mentioned standards and frameworks are being used. For that, the authors identified relevant case studies published in the scientific literature and will discuss them in the following sections.

2. Risk Assessment

Risk assessment is a nuclear procedure to assess cyber resilience. It aims on identifying the threats facing by existing systems (e.g., information systems, communication networks and data repositories) and envisage the potential consequences if adverse events occur. According to the ISO/IEC Information Security Risk Management (ISO/IEC 27005), risk assessment comprises three components: (i) risk identification; (ii) risk analysis; and (iii) risk evaluation. Considering the compilation of the organizational information assets, these tasks aim to identify the threats and vulnerabilities applicable to each asset, considering any controls already setup to assign impact and likelihood values based on risk criteria, to evaluate each risk against predetermined levels of acceptability, and to prioritize which risks need to be addressed, and in which order.

In the scientific literature it is possible to identify case studies published during the last years that were focused on risk assessment [7-10]. One of the identified concerns is the complexity of the risk analysis of complex systems (e.g., industrial control systems), where there is a wide variety of different components and different spatial and temporal scales, as well as fragilities and weaknesses arising from human-in-the-loop. These complex systems might have their functionality severely disrupted if they are exposed to external attacks, which can be physical only, cyber only and blended attacks (i.e., cyber-enabled physical attack and physical-enabled attack) [10]. Considering that the existing methods to assess vulnerabilities in physical and in cyber worlds do not include the interactions and the interdependences that exist in a cyber-physic system, the study reported by article [10] developed a prototype of a new Physical and Cyber Risk Analysis Tool (PACRAT) that can explore the interactions between both the physical and the cyber domains. Moreover, a study focused on smart grids [9] proposed an approach using an inductive modelling technique called event trees, which was used to analyze the impact in the relevant components of a smart grid in terms of confidentiality, integrity, and availability.

Security attacks can condition business continuity and might have an impact propagation factor. Therefore, an incident in secondary or peripheral components might have important and unexpected consequences if it propagates to key parts of the main system [7]. Since in their opinion the general-purpose methods for risk assessment are not suitable to address this problem, the authors of [7] proposed a qualitative dependency (QualTD) model and technique

to be used in addition to the regular risk assessment methods. This proposal was assessed by conducting a risk analysis in the authentication and authorization systems of a large multinational company and it was found that it better estimates and reduces the number of subjective decisions taken by the risk assessor [7].

Moreover, the study reported by [8] was also focused on the risk propagation and aggregation within complex systems and developed a new method, using, as starting points, the individual components of the system being assessed. Having realized that the choose of controls also lack automatic decision support, the authors also proposed evolutionary programming for automating the selection of an optimal set of cyber resilience controls, which minimizes residual risk [8].

3. Risk Management

According to Simon and Brooks [11], "Security risk management provides a means of better understanding the nature of security threats and their interaction at an individual, organizational, or community level".

Although the ISO/IEC Information Security Risk Management (ISO/IEC 27005) does not specify any particular risk management method, it does imply a continual information risk management process that, in addition to the already referred risk assessment components (i.e., risk identification, risk analysis, and risk evaluation), includes more four components (Fig. 1): (i) contextualization; (ii) risk treatment; (iii) communication and consultation; and (iv) monitoring and review.

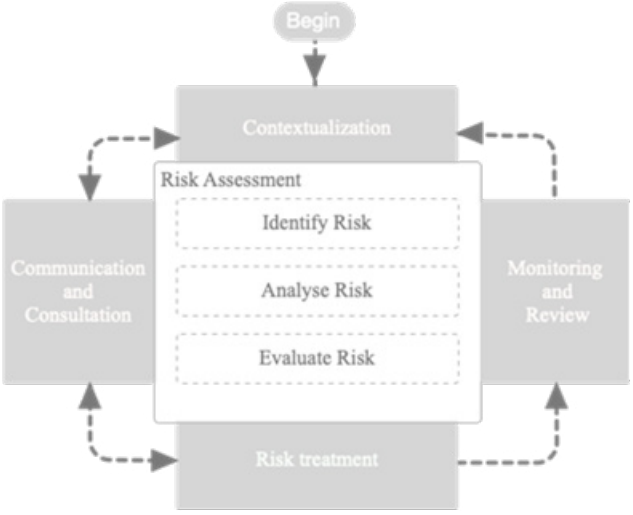

Fig. 1. Risk Management (adapted from ISO/IEC 27005).

Contextualization constitutes the first component of risk management and aims to set the criteria for how risks are identified, who is responsible for risk ownership, how risks impact the confidentiality, integrity, and availability of the information, and how risk impacts and likelihood are calculated.

Risk treatment occur after the risk assessment and four approaches are envisaged: (i) avoid - eliminating the risk; (ii) modify - applying security controls; (iii) share - sharing the risk with a third party (e.g., insurance or outsourcing); and (iv) retain - assuming the risk if it falls within established risk acceptance criteria. In terms of risk acceptance, organizations should determine their own criteria for risk acceptance that consider existing policies, goals, objectives, and shareholder interests.

Finally, communication and consultation should support an effective communication in all the risk management process, while monitoring and review aims to quickly identify changes and maintain a complete overview of the risk picture.

One important thing about risk management is its nature of being iterative, conducted in successive loops. This loop nature is adapted to the needs of a cyber resilience status in the ever-growing IoT environments. Therefore, there is the need for methods and tools to achieve an effective, continuous, and, as much as possible, automated, risk management. In this respect, the case study reported by [12] used NIST special documents (i.e., NIST SP-800-30, NIST SP-800-37, and NIST SP-800-39) and the NIST Risk Management Framework (NIST-RMF) to deal with the cyber resilience of a photo voltaic power plant. The authors explored all the necessary factors to determine risk, such as system characterization, threat identification, vulnerability identification, control analysis, likelihood, and impact analysis [12].

In turn, using NIST SP 800-53 as a guidance, the case study reported by [13] focused on a complex scenario, for which the authors claimed there is no holistic approach to the continuous risk assessment. The scenario included smart-grid's components, deployed in the cloud and a set of IoT resources in a real environment. The objective of the case study was to present a method for continuous risk management, which is based on the use of attack defense trees to capture the relationships between threats and defenses in geographically distributed smart grid's components [13].

4. Frameworks

A cyber resilience framework is more than just a standard. Its purpose is twofold: (i) to help users understand the status of their organizations in terms of being able to prevent, respond and recover their normal business activity (e.g., assess their maturity); and (ii) to guide those users through the process of implement or refine resilience plans. Therefore, cyber resilience frameworks might be considered as guides that organizations may voluntarily implement to merge and align their practices with existing cyber security standards.

Looking specifically to the implementation of well-known frameworks, it is possible to identify several case studies [14-16].

Article [14] reported on the assessment of the cyber resilience of an Indonesian Bank, using C2M2. The assessment was done only in the workforce domain, one of ten domains included in C2M2 framework. This domain was considered by the authors as a key domain for financial institutions, in terms of cyber resilience.

In turn, article [15] reported on the use of the NIST-CSF to assess the cyber resilience posture of a local government organization in Australia. In this study [15] the authors presented a questionnaire aiming to investigate what was the organization's understanding of cyber security risks, considering three categories of participants (i.e., executive, management, and technical participants). Together with the questionnaire the team also defined quantitative and qualitative criteria for each question, sub-category and category and a score system for the various NIST-CSF core functions. Apart from NIST-CSF, additional questions were introduced to help the identification of the desired cyber resilience tier, where the organization wanted to be. As a result, a set of numeric values were achieved, and a set of recommendations were made to improve the various NIST-CSF's core functions [15].

The same NIST-CSF framework was used in the study reported by [16], which intended to assess the cyber resilience status of a hospital and to conclude about the applicability of the referred framework in this kind of organization. In this specific case study, the Cyber Resilience Review (CRR) from the CERT-RMM was used together with the related cross reference tool to frame the answers back to NIST-CSF and identify areas for improvement [16]. The CRR application guidelines were slightly adapted to the real situation, and it proved to be an important out of the box tool to use with NIST-CSF [16].

Moreover, cyber resilience can also be assessed without implementing a particular framework, as is the case of the assessment of a waste-water treatment facility presented by [17].

5. Novel Frameworks and Tools

Despite the existence of standardized frameworks, significative research is focused on the development of new frameworks and tools to assess cyber resilience [18-22].

The authors of [18] were concerned about cyber-physical systems and entry-points that enable cyber-attacks. Considering cyber resilience as a key property of cyber-physical systems, the authors investigated a general-purpose quantitative tool to process experimental data such as the resilience indexes extracted from system logs [18]. Mathematical models based on figure of merit functions were applied on a real wastewater facility considering

simulated attacks, and the achieved metrics were compared with the existing scientific literature [18]. As future work, the authors suggest the validation of the possibility of summarizing cyber resilience through numerical indexes by analyzing data from real systems [18].

Article [19] proposed a new framework that includes a progression model and prioritization policies together with the Cyber Resilience Self-Assessment Tool (CR-SAT) to assess cyber resilience in Small and Medium Enterprises (SME). The authors argued that existing frameworks are too expensive to implement in an environment like the one that characterizes SME, where there is lack of experience in implementing cyber resilience schemas, namely in terms of human resources dedicated to cyber resilience. A field study allowed to gather qualitative results, and the authors concluded that the tool potentially helps SME in their objectives, although other important aids, such as cyber resilience providers, should be considered [19].

Whereas article [19] was focused on SME, the study reported by [20] focused on larger organizations, where subcomponents can have their own cyber resilience strategies. The goal was to derive a strategy to show the overall efficiency and status of cyber resilience in an organization by detecting gaps and overlaps in the cyber resilience schemas of its subcomponents. As a case study, six subcomponents of the Department of Army (DOA) of the United States where considered, but the authors referred in their conclusions that it was a small number: “the convenience sample offers a narrow insight into overall DOA” [20]. The approach was conducted in two phases. In the first phase an interview was made to the representant of each of the six subcomponents, and a qualitative four-by-four resilience matrix was built. In the second phase a cosine similarity analysis was conducted over the matrix to extract information about the alignment (e.g., similarity) of their components. The conclusions, despite of the study limitation, referred positive aspects of the approach in identifying ways of coordinate cyber resilience through all subcomponents of a large organization [20].

A new toolset called Resilience Verification Unit (RevRun) was presented in [21]. The toolset was developed to assess cyber resilience of the architectures of nuclear power plants. RevRun toolset extracts and process data from a simulator, the SCEPTER, developed by Sandia National Laboratories from United States, to produce quantitative resilience metrics [21]. In turn, SCEPTER operates with supervisory control and data acquisition (SCADA) protocols and provides a cyber-physical environment to analyze how cyber-initiated events affect the physical world by using an underlying network emulation and analytics platform to model, simulate, emulate, assess, and validate security systems and processes [21].

Moreover, article [22] reported on methods to extract quantitative measures to support cyber resilience of smart grids. This article also discussed the state estimation software’s resilience under a cyber-attack and concluded that there is a non-linear nature of the resilience status [22]. Therefore, the authors proposed a specific scale, the General Resilience Metric, which considers the controls in place and the systems’ properties such as reliability, security, flexibility, or vulnerability. As a case study it was selected a state estimation software called OTSENKA, developed at the Melentiev Energy Systems Institute from Russia Academy of Sciences. One of the main responsibilities of this software is to continuously monitor SCADA systems looking for data errors or non-conformities [22].

6. Conclusion

Based on the analysis of case studies, this survey has identified different approaches towards the goal of a cyber resilient status, and therefore, to improve the business-continuity of various kinds of organizations.

One identified approach focused on risk assessment and risk management processes and the complexity of their implementation. Some studies argued that the complexity in risk assessment is related to the existence of a considerable number and variety of components contained within the systems. Also contributing to the complexity of risk assessment some studies reported on case studies focused on systems with a great danger of risk propagation, from the peripheric components, not directly connected to high-risk situations, to the system’s core components, thus reaching important targets. In maintaining some degree of cyber security status, the risk management process must produce an up-to-date picture of risk related information in the organization. Some studies focus on improving the cyclic nature of risk management process, introducing new tools and methods to build and maintain an up-to-date risk overview.

A different approach focused on the implementation of frameworks to assess cyber resilience. In this respect, some studies reported the use of well-known frameworks (e.g., NIST-CSF or C2M2) whereas others propose new frameworks and tools to deal with this assessment. The implementation of cyber resilient plans, guided by frameworks,

imply the need to go through questionnaires that are adaptable to the organizations' profiles. Different studies report diverse ways to tackle with this problem (e.g., CRR or ad-hoc questionnaires).

Aside from the well-known frameworks, there were some studies reporting proposals for new ways of cyber resilience assessment. They argued that due to the complexity in the structure of large organizations (e.g., DOA), or the lack of resources (e.g., SME), new methods to support the assessment of cyber resilience are needed. Moreover, other studies presented new methods to have a quick and updated report on the cyber resilience status of some organizations, heavily supported on electronic components (such as cyber-physic), since the underlying infrastructures of these kind of organizations allow the automatic extraction of data necessary to build cyber resilience indicators.

The identified case studies focused on different contexts, including critical organizations like banks, hospitals, power plants, smart grids, industrial control systems, public administration, small and medium enterprises, and information technology providers.

It seems that the search for guidance in the processes that conduct organizations to a cyber resilient state is a general worry. In complement to well-known cyber resilience frameworks, which are abstract and open enough to be easily adaptable to different organizations and profiles, new frameworks had been proposed. Although there are reports on the applicability of existing frameworks, new methods are needed to either complement or replace parts of those frameworks, due to the complexity of the underlying systems, which has two different natures: (i) the structural nature, that comes from the fact that organizations are sometimes too complex such is the case of large organizations with many departments that co-exist with a certain degree of independence (i.e., sub-components); and (ii) the genetic nature that points to the kind of components that compose an organization. In this case the complexity comes from the fact that the business is based on diverse electronic components with distinct characteristics, able to automatically feed risk assessment and cyber resilience indicators to appropriate algorithms.

The most prevalent international standards naturally do not necessarily promote the use of a specific type of risk assessments, there has been a tendency to advocate the use of qualitative risk analysis as even stated in the ISO/IEC Information Security Risk Management (ISO/IEC 27005): "In practice, qualitative analysis is often used first to obtain a general indication of the level of risk" [23]. When considering qualitative methods, experts' intuition and subjectivity are involved. Moreover, using scoring methods that plots risks on a matrix has drawbacks related to the ambiguity in meanings and inconsistencies in risk analysis. In fact, words easily misinterpreted or carrying different meanings leave organizations vulnerable to potential risks.

Therefore, it is predictable that different directions for cyber resilience will be considered to shift from purely qualitative judgments to quantitative models that leverages measurements. In this respect, special attention should be given to the methods and tools proposed by Factor Analysis Information Risk (FAIR), the only international standard quantitative model, for understanding, analyzing, and quantifying cyber and operational risk in financial terms [24], that usually involves Monte Carlo simulations to express probability distributions.

References

[1] Social Media Users Pass The 4.5 Billion Mark, https://wearesocial.com/uk/blog/2021/10/social-media-users-pass-the-4-5-billion-mark/, last accessed 2022/6/19

[2] Bilotta, S., Nesi, P. (2022) "Estimating CO2 emissions from IoT traffic flow sensors and reconstruction." *Sensors* **22(9)**: 3382.

[3] Gonçalves, G.D.L., Filho, W.L., Neiva, S.D.S., Deggau, A.B. et al. (2021) "The impacts of the fourth industrial revolution on smart and sustainable cities." *Sustainability* **13(13)**: 7165.

[4] Campo, G.D., Calatrava, S., Canada, G., Olloqui, J., Martinez, R., Santamaria, A. (2018) "IoT solution for energy optimization in industry 4.0: Issues of a real-life implementation." In *2018 Global Internet of Things Summit* (GIoTS 2018), Piscataway, New Jersey, IEEE.

[5] Shoemaker D., Kohnke, A., Sigler, K. (2019) *How to Build a Cyber Resilient Organization*, CRC Press.

[6] Stallings, W. (2019) *Effective Cybersecurity, Understanding and Using Standards and Best Practices*, Pearson Education, Inc.

[7] Zambon, E., Etalle, S., Wieringa, R.J. et al. (2011) "Model-based qualitative risk assessment for availability of IT infrastructures." *Software System Model* **10**: 553–580.

[8] Kavallieratos G, Spathoulas G, Katsikas S. (2021) "Cyber Risk Propagation and Optimal Selection of Cybersecurity Controls for Complex Cyberphysical Systems" *Sensors* **21(5)**: 1691.

[9] Langer, L., Smith, P., Hutle, M. and Schaeffer-Filho, A. (2016) "Analysing cyber-physical attacks to a Smart Grid: A voltage control use case." In *Power Systems Computation Conference (PSCC)*, Piscataway, New Jersey, IEEE.

[10] D. MacDonald et al. (2013) "Cyber/physical security vulnerability assessment integration." In *IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*, Piscataway, New Jersey, IEEE.

[11] Smith, C. and Brooks, D. (2013) *Security Science: the theory and practice of security*, Elsevier.

[12]. Miranda, A.W. and Goldsmith, S. (2017) "Cyber-physical risk management for PV photovoltaic plants." In *International Carnahan Conference on Security Technology (ICCST)*, Piscataway, New Jersey, IEEE.

[13]. Rios, E., Rego, A., Iturbe, E., Higuero, M. and Larrucea, X. (2020) "Continuous Quantitative Risk Management in Smart Grids Using Attack Defense Trees." *Sensors* **20(16)**: 4404.

[14] Putra, A.P.G., Humani, F., Zakiy, F.W., Shihab, M.R., Ranti, B. (2020) "Maturity Assessment of Cyber Security in The Workforce Management Domain: A Case Study in Bank Indonesia." In *International Conference on Information Technology Systems and Innovation (ICITSI)*, Piscataway, New Jersey, IEEE.

[15] Ibrahim, A., Valli, C., McAteer, I. et al. (2018) "A security review of local government using NIST CSF: a case study." *J Supercomput* **74**: 5171–5186.

[16] Pereira, B., Pavão, J., Carreira, D., Costa, V., Rocha, N.P. (2022) "A Security Review of a Portuguese Hospital Using the Cyber Security Framework: A Case Study." In: Antipova, T. (eds) *Digital Science. DSIC 2021. Lecture Notes in Networks and Systems*, 381, Springer.

[17] Murino, G. and Tacchella, A. (2018) "Concrete vs. Symbolic Simulation to Assess Cyber-Resilience of Control Systems." In *European Conference of Modeling and Simulation (ECMS)*, ECMS.

[18] Murino, G., Armando, A., Tacchella, A. (2019) "Resilience of Cyber-Physical Systems: An Experimental Appraisal of Quantitative Measures." In *11th International Conference on Cyber Conflict (CyCon)*, Piscataway, New Jersey, IEEE

[19] Carías, J.F., Arrizabalaga, S., Labaka, L., Hernantes, J. (2021) "Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs." *IEEE Access* **9**: 80741-80762.

[20] Wood, M.D., Wells, E.M., Rice, G., Linkov, I. (2019) "Quantifying and mapping resilience within large organizations." *Omega* **87**: 117-126.

[21] Galiardi, M., Gonzales, A., Thorpe, J., Vugrin, E.D., Fasano, R.E., Lamb, C. (2020) "Cyber Resilience Analysis of Scada Systems in Nuclear Power Plants." In *International Conference on Nuclear Engineering*, vol. 83778, New York, American Society of Mechanical Engineers.

[22] Voropai, N., Kolosok, I., Korkina, E. (2018) "Resilience Assessment of the State Estimation Software under Cyber Attacks." In *E3S Web Conference*.

[23] Hubbard, W., Seiersen, R. (2016) *How to Measure Anything in Cybersecurity Risk*, Wiley.

[24] Freund, J. and Jones, J. (2015) *Measuring and Managing Information Risk - A FAIR Approach*, Elsevier.