International Scientific Conference
CONTEMPORARY ISSUES IN BUSINESS, MANAGEMENT AND ECONOMICS ENGINEERING 2021
13–14 May 2021, Vilnius, Lithuania
Vilnius Gediminas Technical University
eISSN 2538-8711
eISBN 978-609-476-260-4
Article ID: cibmee.2021.611
https://doi.org/10.3846/cibmee.2021.611

CYBER SECURITY MANAGEMENT MODEL FOR CRITICAL INFRASTRUCTURE PROTECTION

Manuela TVARONAVIČIENĖ[1], Tomas PLĖTA[2*], Silvia DELLA CASA[3]

[1, 2]Department of Business Technology and Entrepreneurship, Faculty of Business Management, Vilnius Gediminas Technical University, Saulėtekio al. 11, LT-10223 Vilnius, Lithuania
[1]Daugavpils University, Parades Str. 1-421, LV-5401 Daugavpils, Latvia
[3]NATO Energy Security Centre of Excellence, Šilo g. 5A (K-22), LT-10322 Vilnius, Lithuania

Received 09 February 2021; accepted 01 April 2021

Abstract. *Purpose* – in this article, the authors propose a management model for Critical Infrastructure cybersecurity, further development of a model developed by Limba, Plėta, Agafonov, and Damkus (2017).

Research methodology – methodology consists of researching the best practices in cybersecurity management for Critical Infrastructures and evaluating the best element to be included. The article offers an overview of the model, including structure and objectives, and further analysis that focuses on pre-existing CI management frameworks.

Findings – main results show that, although previously published protocols and models contain valuable elements, there is still the need to implement a comprehensive model which can be applied to every type of CI.

Research limitations – research might have been limited due to the lack of a unitary approach to cybersecurity management for CI, meaning the lack of possibility of reference to a similar model and approach.

Practical implications – model which is presented in the article could offer a new approach to CI protection strategies and could be the beginning of a more structured approach towards their protection.

Originality/Value – model was created by the authors with references to past published protocols and models, which are present in the quotation in the text as well as the bibliography.

Keywords: critical infrastructure, management, cyber-attack, energy security, cybersecurity.

JEL Classification: M15, Q48.

Conference topic: Business Processes: Development, Digitalization, Social Responsibility.

Introduction

With the development of newer power systems in Critical Energy Infrastructures (CEI), there has been a shift in the management required to ensure cybersecurity in Industrial Control Systems (ICS). While initially, such systems were part of the Operational Technology (OT) environment, with digitalization a merge occurred between OT and Information Technology (IT) environment (Drias et al., 2015; Das & Gunduz, 2019). The introduction of smart devices in different layers of production and communication within an organization brought great innovation, but also a higher risk for cyber-based attacks (Pandey & Misra, 2016). For this, it is needed the development of a new type of management model which can be appliable to every type of CEI, which can ensure cybersecurity for such different systems. The article aims to develop a new type of management model which focuses on the cybersecurity of CIs and ensures full protection of all of the types of Cis. It is important to remember that there is not a possible "one solution fits all" model, as each company or organization possesses different types of infrastructures and technical aspects (Plėta et al., 2020a; Technical Committee ISO/IEC JTC, 2013). The article will then employ a scientific analysis that takes from pre-existing frameworks regulating cybersecurity management, such as the COBIT 2019 model offered by the global association ISACA (ISACA, 2018). An additional model that is referenced is the *Cybersecurity Management Model for Critical Infrastructures* developed by Limba, Plėta, Agafonov, and Damkus (2017). The methodology that is used in the article comprehends two major parts: the analysis proposes a management model employed for the protection of Critical Energy Infrastructures, including their vulnerabilities in the case of cyber-attacks.

*E-mail: *Tomas.Pleta@vilniustech.lt*

The second part of the analysis focuses instead on the development of an adequate management framework for the protection of renewables, which considers the development of a new set of criteria upon which it is possible to determine the level of vulnerability in the provision of renewable energy. The model itself is the further development of the model proposed by Limba et al. (2017), while in the second part interesting elements from pre-existing models will be taken into consideration as a potential part of the new model. The application of such a model is meant to be considered by governmental agencies or international organizations that want to develop an accurate list of different types of CI by the level of security: given that the model is supposed to be appliable to every type of Critical Infrastructure, and then in a second time integrated with more type-specific protocols, it could accurately depict the security within a CI by the same categories and hence having a more comprehensive vision of the effectiveness of cybersecurity strategies. The methodology implies an analysis of recognized best practices in the field of cybersecurity management techniques, and takes into account the most universal elements, which can be considered suitable to every type of CI, and then offers a new model which can be used to achieve a more prioritized evaluation of security within a state or a group of states. Throughout the research, a few problematic points were recognized as poignant for the development of the model, such as the fact that currently there is no account for a generalized set of norms or regulations for CI protection. The approach that was seen in various protocols differed as well in terms of management concepts, of definitions of key elements such as cybersecurity, threat, and ultimately the various classification of vulnerability and level of risk. For this reason, it was complex to evaluate a middle way in the development of the model's category.

The development of an effective cybersecurity model has been a challenge for many researchers in various countries, as it represents a crucial point at both domestic and crucial levels. It is important to note that already the European Commission has presented a CIP dissemination network, which allows the exchange and share of information and best practices by public authorities, private sector representatives, and experts (European Commission, n.d.), following the practices of the United States in the *Critical Infrastructure Threat Information Sharing Framework* (Cybersecurity and Infrastructure Security Agency, 2013, 2016). The peculiarity of Critical Infrastructure protection is due to the complexity of its structure, which has been the consequence of the merging of IT and OT environments for Industrial Control Systems (Plėta et al., 2020a). The development of the Internet of Things (IoT) and the consequent dependency of ICS on the latter has raised the risks faced by CEI, with Operational Technology (OT) environments as the growth targets of attacks, such as water systems, energy plants, transportation, communication, critical manufacturing i.e. (DRAGOS, 2017).

1. Cyber Security Management for Critical Infrastructure

As mentioned in the introduction, this part of the article is dedicated to the proposal of the management model targeting Critical Infrastructure protection, which is the continuation of the model developed by Limba et al. (2017). The description of the model is not performed in-depth, but instead offers a general overview of its core components and the relationship between categories, along with some elucidation of the classification choices and motivations. Other sources that have been considered in the redaction of this model are previous works of the authors, including the articles *Cyber-attacks to critical energy infrastructure and management issues: overview of selected cases* (Plėta et al., 2020a), *Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA*, *UK*, *France*, *Estonia and Lithuania* (Tvaronavičienė et al., 2020), and *Cyber effect and security management aspects in critical energy infrastructures* (Plėta et al., 2020b). In terms of the development of the concept of security and awareness within an enterprise, other articles that were useful for the research were *Training in shaping employee information security awareness* (Stefaniuk, 2020) and *Organizational security culture in small enterprises: a case study* (Gierszewski & Pieczywok, 2020).

The concept of cybersecurity considered for this model follows the *CIA Triad*, which is comprised of three major objectives: *confidentiality*, meaning the protection of sensitive information from unauthorized access; *integrity*, meaning the protection of data from unauthorized access, and finally *availability*, meaning that the systems' mechanisms are available in emergencies (Forcepoint, 2020). Having this in mind, it is important as well to clear that the structure and core principles of the model will be appliable to every type of CEI to achieve cybersecurity, and considers the advancement of new technologies as an integral part of the model. However, the model as well considers the *n*-1 principle for technology: although the model promotes the newer technology for ICT systems to rely on, it is considered better to rely not on the latest versions, but to have to rely on older generation technology for stability. Having clarified these aspects, the following part of the text will go into detail in describing the core principles of the proposed model.

The model structure can be summarized in the following way:

As it is shown in Figure 1, the model consists of *seven* core categories appliable to every type of CEI, which are:

– Resources Management: the first category of the model, and probably the most important, describes the skeleton of the system to whom the model is applied to. Agencies need to know all of the elements which are part of their physical system and to be aware of their vulnerabilities and weak links of their existing security systems (GEANT, 2019). This category should for this reason be one of the first to be considered in the implementation

Figure 1. Cyber security management model for critical infrastructures
(source: made by the authors)

of the model since it is particularly useful in the preparation of the rest of the categories, but it is also useful for the process of monitoring the modifications to the system. This category aims to determine the state of security of the system, by assessing the physical security of the infrastructure and considering the physical assets of the CI, by determining the modalities of access control used in the facility, and finally the classification of the vulnerabilities of the establishment.

– Organizational Management: This category provides insights on the guidelines to be used in the direct response to cyber-attacks, which is of the utmost importance in emergencies. The focus on the category is mostly on the aftermath of the attack, namely the Disaster Recovery Planning, which comprehends the general instruction on how to behave in the various scenarios post-cyber-attack. Moreover, it offers a focus as well on Operational Security, which clarifies various techniques employable for the prevention and the response to cyber-attacks.
– Technology Management is another important category for the model, as it determines the cybersecurity of software, telecommunications, and network. While the Organizational category treated the physical security of the infrastructure, in this case, the focus is on the quality of the IT environment employed, with the implementation of various cybersecurity techniques, which will be varying according to the type of software and infrastructure the model is applied to.
– Cyber Culture Management category deals with the informational aspects of cybersecurity, as well as the "human" part of the system. It is the priority of this category to determine the safety of the employees as well as to raise awareness and training the staff to understand the basics of cybersecurity management.
– Legal Management is without a doubt an interesting addition to the model, as it gives the possibility of incorporating a pre-existing framework to the model: since the latter is qualified to apply to every type of CI, such category is needed to add to each model more specific characteristics and recommendations.
– Security Management: the aspects treated in this category are focused on cyber incident management, which means the guidelines to develop an effective management plan to be applicable in an emergency, and which covers every aspect of the event, from the preparation to the identification and handling, as well as the follow-up. The category will as well offer more information on the planning for other non-cyber-related consequences such as physical incidents and safety management.
– Strategy Management deals mainly with the techniques employed by the model in general, such as the calculations, as well as the detection of other present CEI that may be linked to the one to which the model is applied to.

2. Analysis of pre-existing management models of CEI protection

As it was mentioned before in the text, the thesis proposed by the article is to demonstrate the validity of the application of a management model for CEI. The analysis which is conducted in the article will consider various pre-existent management models for cybersecurity and will evaluate their efficiency in protecting CEI, especially considering the

implementation of newer techniques employed by such systems as big data analysis. The first framework that is taken into consideration for the analysis is the *COBIT 2019*, a framework developed for the governance and the management of IT, aimed at whole enterprises (ISACA, 2018). The further analysis considered as well the *NERC Implementation Guidance for CIP-008-6* (North American Electric Reliability Corporation [NERC], 2019), which aims to determine the incident response plan to cyber-based attacks in enterprises, as well as classification and prevention of damage from the management point of view. Another important framework that was taken into consideration is the *NIST Guidelines for Smart Grid Cybersecurity* (National Institute of Standards and Technology [NIST], 2014, 2018), which serves as a national-level framework that can be applied to multiple sectors, and is a further evolution of Critical Infrastructure Protection (CIP). Another important management model that is taken into consideration is the *Cyber Security Management Model for Critical Infrastructure* developed by Limba et al. (2017), which is concerned with technological aspects used for CIP from cyber-based attacks and vulnerabilities. The analysis in the paper is presented in the following way: every mentioned document is presented with a short paragraph that considers the elements of such a framework that could be part of an adequate management model for CEIP. Rather than explaining extensively the contents of each document, the focus is on the parts that the authors considered to be necessary to develop such a framework. Particular attention is made concerning the solutions to vulnerabilities linked to the aforementioned advanced techniques in CEIP such as AI or ML. The final step of the analysis will be the development of an additional series of criteria that might be integrated into the aforementioned framework for CEIP.

3. Categories evaluation: responsibilities, processes, and third-party services

The main framework that was used in the analysis is the *COBIT 2019*, developed by ISACA as a framework that aims to develop and promote the process of understanding, designing, and implementing "*enterprise governance of IT"* (*EGIT*) (ISACA, 2018). The framework is periodically reviewed, as the one considered for this article is the one used in 2020, which was published in 2018. The framework offers an interesting take on the possible governance and management of IT aimed at enterprises, which can be applied in various branches of the latter. There are a few elements that are used by this framework that are particularly suitable for developing a management framework of CEI, although as mentioned before, this document offers a model that can manage various aspects of an enterprise (ISACA, 2018). It is important to mention that, at the beginning of the document, a differentiation is made between the concept of *governance* and *management*: the first is considered a responsibility of the board of directors, which then sets directions that are followed in *management* plans, which are considered responsibilities of the executive management under the CEO of the enterprise (ISACA, 2018). This offers valuable insight into the *responsibilities* within an enterprise and renders the response to emergencies much quicker.

Furtherly, the *COBIT Components of a Governance System* represents a useful tool for the classification, preparation, and management of an enterprise's core elements (ISACA, 2018). The criteria which are used to characterize the *Governance System*, according to *COBIT*, are seven: *a) Processes*, *b*) *Organizational Structures*, *c*) *Services*, *Infrastructures*, *and Applications*, *d*) *Principles*, *Policies*, *Procedures*, *e*) *Culture*, *Ethics*, *and Behaviour* and *f*) *Information* (ISACA, 2018). The criteria which were found particularly useful for the purposed of the model are firstly *a*) *Processes*, which possess a rating system with whom are evaluated the capabilities level for each process: the range goes from 0, which represents the absence of any basic capability, to 5, which represents the full achievement of the process' purpose (ISACA, 2018). This aspect was taken as a possible system of classification of the enterprise's pre-existing systems and elements, given that a complex classification usually is more adequate in case of emergencies, because an enterprise that knows all of its components knows as well all of its vulnerabilities. Another interesting category which was taken into consideration is *b*) *Organizational Structures:* the model offers a wide classification of various roles within the enterprise, not only by defining their role in the company but classifying them in a system that considers their different levels of *responsibility* (who drives the task?) and *accountability* (who accounts for the task's success?) (ISACA, 2018). A culture of security can be seen as *"behaviour and relations of individuals and employee teams*, *in courts and attitudes*, *in the way problems and conflicts are solved*, *work organization and human interaction"* (Gierszewski & Pieczywok, 2020). As the aforementioned classification is considered as a way to improve the security of an enterprise, the development of a system clarifying *roles* and *responsibilities* would improve the quickness of response as well in terms of identifying the vulnerable elements of the system in case of cyber-based attacks (Bhat et al., 2013). Another important element of the *COBIT* model is represented by the category *d*) *Principles*, *Policies*, *Procedures:* the model proposed by ISACA reserves an additional category, which consists of adding to any process the possibility to reference a particular process or additional framework as a *third-party service*, by integrating it to the existent model. This solution is a great approach to consider in developing an effective model, given that these additional protocols or frameworks can change and evolve with time, and consequently modernize the "base" framework. These elements offered by the *COBIT* framework are fit for the model concerning CEIP, hence they are taken into consideration for the final model.

4. Classifications of cyber incidents

Another important document that was considered for the analysis was the *NERC Implementation Guidance for CIP-008-6*, published by the North American Electric Reliability Corporation in 2018 (NERC, 2019). The document is mainly used, as it is said in the title, for the North American electricity systems, aiming in particular to CIP. The document offers useful insights for CIP and possesses an approach that is based on the response of cyber-based incidents or attacks in CI. An interesting element within the framework is the *Classification of Cyber Incidents:* as the classification of an enterprise's elements is useful for preventing a cyber-attack, a system that evaluates an enterprise's vulnerabilities can help in developing appropriate responses and solutions to various situations. The classification of cyber-incidents offered by the *NERC* system comprehends 6 levels, *Baseline* (*0*), *Low* (*1*), *Medium* (*2*), *High* (*3*), *Severe* (*4*), and *Emergency* (*5*), and is based on the attack's consequences (NERC, 2019). Besides, such classification provides as well a reportability threshold, by which only incidents with a level superior or equal to 3 are reportable to the responsible authorities: this prevents an overcharge of aid requests within an enterprise. Moreover, the other interesting element which was found within the framework is the role of the *E-ISAC/ NCCIC Reporting Coordinator*, which is responsible for the coordination of regulatory reporting activities related to E-ISAC (Electricity Information Sharing and Analysis Center) and the NCCIC regulatory framework (NERC, 2019). The role of such authority within an enterprise is to determine the need to contact third-party services or international authorities in case of a severe cyber-attack and could be useful for the security of the enterprise. As it was reported in the article by Plėta et al. (2020a) on cybersecurity management aspects, the NERC framework relies on the NIST guidelines; the introduction of the classification of Cyber Incidents based on a risk-assessment method could be a valid technique to develop in a general model (Plėta et al., 2020a).

5. Cryptography and digital certificates

The *NIST Guidelines for Smart Grid Cybersecurity* is a sector-specific management framework dedicated to North American Smart Grid systems, developed by the National Institute of Standards and Technology (NIST) in 2014 (NIST, 2014). Although the model developed within the article is targeted to all types of CEI, this document provides an interesting take on key management techniques: smart grid systems possess more advanced technology in security systems, with the aforementioned implementation of big data analysis. Hence, the document offers a more up-to-date type of technology management solutions in terms of security requirements. The mentions in the document are a few and include the employment of *symmetric ciphers* for authentication and encryption, *public-key cryptography*, which needs to be supported by a hardware (cryptography co-processor) or in software (NIST, 2014). Additionally, the employment of *public-key certificates*, which are *"bind user or device names to a public key through some third-party attestation mode"* (NIST, 2014).

6. Cyber Security Management Model for Critical Infrastructure

The model developed throughout the article is the further development of the article by Limba et al. in 2017, the *Cyber Security Management Model for Critical Infrastructure* (Limba et al., 2017). The model was originally developed specifically for CIP from cyber/based attacks, in particular relating to the security of Industrial Control Systems (ICS). The interesting aspect offered by the model is that it offers an insight into the development of the ICS in terms of protection: although ICS were considered part of the Operational Technology (OT) security, further digitalization of industrial technology brought the merging of Informational Technology (IT) and OT systems for ICSs. An issue highlighted by the authors is that, given the merging of OT and IT technology, it is needed for ICS to develop a security model that considers both environments, including a supply management system that can sustain cybersecurity aspects (Limba et al., 2017). Moreover, the model proposed by Limba et al. (2017) is particularly focused on the technology management aspects of cybersecurity, which is mentioned in one of the six categories developed, *technology management*: the text describes the latter as the understanding and classification of each component of the enterprise, and the consequent vulnerabilities (Limba et al., 2017). Considering this element, there could be an evolution of the category in terms of the effectiveness of each technique used for technology management, including big data analysis: hence, it can be useful for the analysis.

7. Elements to take into consideration from pre-existing models

Given the previous overview of different preexisting management models for CEI, this part of the article will be dedicated to the proposal of a management model for cybersecurity that can be used for all types of CEI. The ultimate aim of the model is to achieve an adequate level of cybersecurity. The aforementioned analysis provided useful insight on some elements which were integrated into the model made by the authors. The elements which are taken into consideration are:

- Processes, which can be described as the whole set of practices and activities which altogether achieve full cybersecurity. The general definition is taken from the one used in the COBIT 2019 protocol, which for each process appoints one or more activity (ISACA, 2018). The classification of such a process should include all the stages needed for the implementation of an adequate management strategy for implementing cybersecurity, covering the aspects of prevention, intervention, and recovery from a cyber-related threat. Moreover, to classify an enterprise's assets, each process will be assigned a value, which will reflect the level of implementation: the range will go from 0 to 5, in which 0 represents the total lack of implementation and 5 represents the full achievement of the process' purpose (ISACA, 2018). By using this solution, not only the development of a management strategy is easier, but it is immediately noticeable what are a system's flaws and vulnerable points.
- Roles and Responsibilities: as Stefaniuk (2020) puts it, "employees' improper conduct or lack of action lead to the majority of information security incidents" (Stefaniuk, 2020). Hence, this element is highly useful for the organizational aspects of management since the purpose of the latter is to determine and classify the roles within an enterprise, including a short description of the role's priorities. Moreover, this element will relate to the processes described in the previous paragraph, for the roles will each be given responsibility for one or more processes, to speed up the response in an emergency, and to determine the weak links of the systems in such situations. The development of such element should as well follow the directives offered by the COBIT 2019 framework, although it would be useful to develop a specific role for reporting cyber incidents, active at all times, to whom the members of the organization could turn to in the time of need, much like the role of the E-ISAC/NCCIC Reporting coordination mentioned in the NERC framework (NERC, 2019).
- Technology management covers the more technical aspects of management: given that the model targets various types of CEI, this element will be more specifically dedicated to the classification of the technical components used for the enterprise's security, including the types of techniques. This also means that there will be a general classification of security technology techniques applicable to every CEI, and possibly the development of specific sections for CEI types. Moreover, the development of this element will as well have a focus on technical aspects and will offer a classification of the security techniques, which will be ranked in terms of effectiveness and innovation. In this way, a system will gain a higher mark if it possesses newer and effective security technology techniques, however still considering the aforementioned n-1 principle.
- The Policy is one of the most innovative aspects of management modelling: as aforementioned, this model is appliable to every type of CEI, and for the model to be capable to do so, the more specific aspects of security management for every CEI are not mentioned right away. To resolve this issue and still propose an adequate and comprehensive model, there will be an additional category, which will include the implementation of other frameworks relative to the specific CEI to whom the model is applied to. Moreover, for each mentioned CEI there will be the possibility to integrate the model with countless other protocols, which could be substituted as newer versions are published, making the model suitable for long periods.
- The last one is Vulnerabilities, which completes the organizational management aspects: along with processes and techniques employed within the enterprise, it is important as well to consider the possible weak points of the system by testing and classifying the vulnerabilities of the system. By doing this, not only it is easier to develop fast solutions preventively, but it is also a necessary step to not be caught unprepared in emergencies. The element could as well be improved by considering a ranking of vulnerabilities which is based on the consequences of a potential cyber-attack could have to the weak points of the system. In this case, it would be the management's job to determine the cases in which it is necessary to contact official authorities, hence speeding up the process of recovery in case of cyber-attack.

Conclusions

The article proposed a cybersecurity management model applicable to every type of CEI, including the more recent RES. To reach a standardized implementation of such a model would mean easier communication between authorities and entities and would as well focus on the development of new protocols specific for each type of CEI. The major issue in researching and developing such a model was the need to accommodate each category in a suitable way for all types of CI, which was resolved by the development of the Legal Management section. The result of the implementation of the model is useful for both companies wanting to reach an adequate level of security over their information and also, from a national perspective, to assess a plausible list of national CI sorted in order of priority. The latter means that each CI would be evaluated in terms of how much of a threat would be their malfunctioning in case of attack: doing so, there will be a much clearer idea of where to direct most attention in an investment of security, and to recognize which are the weak links of a nation's infrastructures. Moreover, such a process would highlight the interconnectivity of CI, prioritizing the infrastructure whose functioning benefits other CI. Overall, the model aims to raise awareness on the need for CIP, and how much is it necessary to face such a topic on a national level as well as on an enterprise level.

Disclosure statement

The authors do not have any competing financial, professional, or personal interests from other parties.

References

Bhat, K., Sundarraj, V., Sinha, S. & Kaul, A. (2013). *IEEE Cyber security for the smart grid.* IEEE. https://doi.org/10.1109/IEEESTD.2013.6613505

Cybersecurity and Infrastructure Security Agency. (2013). *National Infrastructure Protection Plan* (*NIPP*) *2013: Partnering for critical infrastructure security and resilience.* Homeland Security, Washington DC. https://www.cisa.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

Cybersecurity and Infrastructure Security Agency. (2016). *Critical infrastructure threat information sharing framework.* Homeland Security, Washington DC. https://www.cisa.gov/publication/ci-threat-info-sharing-framework

Das, R., & Gunduz, M. Z. (2019). Analysis of cyber-attacks in IoT-based critical infrastructures. *International Journal of Information Security*, *8*(4), 122–133. https://www.semanticscholar.org/paper/Analysis-of-cyber-attacks-in-IoT-based-critical-Das-G%C3%BCnd%C3%BCz/82ceb54c997b5c779f45ee191012716b4269eb23

DRAGOS. (2017). *CRASHOVERRIDE: Analysis of the threat to electric grid operations.* Hanover. https://www.key4biz.it/wp-content/uploads/2017/06/CrashOverride-01.pdf

Drias, Z., Serhrouchni, A., & Vogel, O. (2015). Analysis of cyber security for industrial control systems. In *2015 International Conference on Cyber Security of Smart Cities*, *Industrial Control System and Communications* (*SSIC 2015*) (pp. 83–91). Shanghai, China. IEEE. http://doi.org/10.1109/SSIC.2015.7245330

European Commission. (n.d.). *Critical infrastructure warning information network*. http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network/index_en.htm

International Organization for Standartization. (2013). *Information technology – Security techniques – Code if practice for information security controls* (Technical Committee ISO/IEC JTC 1). https://www.iso.org/standard/62726.html

Forcepoint. (2020). *The CIA triad defined.* Retrieved November 2, 2020 from https://www.forcepoint.com/it/cyber-edu/cia-triad

GEANT. (2019, September 12). *TF-CSIRT: Computer security incident response teams: Coordinating training*, *services and knowledge-exchange for security teams worldwide.* https://www.geant.org/People/Community_Programme/Task_Forces/Pages/TF-CSIRT.aspx#top

Gierszewski, J., & Pieczywok, A. (2020). Organisational security culture in small enterprises: A case study. *Entrepreneurship and Sustainability Issues*, *8*(2), 438–453. https://doi.org/10.9770/jesi.2020.8.2(26)

ISACA. (2018). *COBIT 2019 framework: Governance and management objectives*. https://www.isaca.org/bookstore/bookstore-cobit_19-digital/wcb19fgm

Limba, T., Plėta, T., Agafonov, K., & Damkus, M. (2017). Cyber security management model for critical infrastructure. *Entrepreneurship and Sustainability Issues*, *4*(4), 559–573. https://doi.org/10.9770/jesi.2017.4.4(12)

North American Electric Reliability Corporation. (2019). *Cyber security – Incident reporting and response planning: Implementation guidance for CIP-008-6.* www.nerc.com/pa/comp/Reliability Standard Audits Worksheets DL/RSAW CIP-008-5_2015_v1.docx

National Institute of Standards and Technology. (2014). *Guidelines for smart grid cybersecurity.* https://doi.org/10.6028/NIST.IR.7628r1

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity.* https://doi.org/10.6028/NIST.CSWP.04162018

Plėta, T., Tvaronavičienė, M., Casa, S. D., & Agafonov, K. (2020a). Cyber-attacks to critical energy infrastructure and management issues: overview of selected cases. *Insights into Regional Development*, *2*(3), 703–715. https://doi.org/10.9770/IRD.2020.2.3(7)

Plėta, T., Tvaronavičienė, M., & Casa, S. D. (2020b). Cyber effect and security management aspects in critical energy infrastructures. *Insights into Regional Development*, *2*(2), 538–548. https://doi.org/10.9770/IRD.2020.2.2(3)

Pandey, R., & Misra, M. (2016). Cyber security threats – Smart grid infrastructure. In *2016 National Power Systems Conference* (*NPSC*) (pp. 1–6). Bhubaneswar, India. IEEE. https://doi.org/10.1109/NPSC.2016.7858950

Stefaniuk, T. (2020). Training in shaping employee information security awareness. *Entrepreneurship and Sustainability Issues*, *7*(3), 1832–1846. https://doi.org/10.9770/jesi.2020.7.3(26)

Tvaronavičienė, M., Plėta, T., Casa, S. D., & Latvys, J. (2020). Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK, France, Estonia and Lithuania. *Insights into Regional Development*, *2*(4), 802–813. https://doi.org/10.9770/IRD.2020.2.4(6)