International Journal of Cyber Operations and Cyber Security Governance
Volume 1 Issue 1, 2026

A Framework for Critical Infrastructure Cybersecurity Management

S. Vijaya laxmi, Sagarvarma, Sarawathi
[1,2,3]Professor, HoD
Department of Computer Engineering

Article Info
Received: 26-02-2026 Revised: 07-03-2026 Accepted: 14-03-2026 Published: 24-03-2026

Abstract. In today's technology-driven world, cyber security is paramount. Information technology is essential to the day-to-day functioning of many organisations, including public and commercial sectors, government agencies, banks, water providers, power grid operators, nuclear power plants, and wastewater treatment facilities. Cybersecurity is essential since all technology relies on communication and information systems. Companies in both the public and commercial sectors continue to remain susceptible despite the millions of dollars spent annually on cybersecurity software, hardware, and technologies. The underlying issue here is that cyber security is still mostly seen as a technological component that can be readily integrated into an organization's operations to provide protection. These days, cyber defence is much more than simply hardware and software. Critical infrastructure attacks are classified in this article, along with the most common cyber security mistakes made by organisations in their efforts to protect themselves from vulnerabilities, attack vectors, and methods. In order to help organisations and businesses secure their vital infrastructure, this essay will primarily focus on the theoretical components of a cyber security management model. Critical infrastructure protection against cyber threats and vulnerabilities is not the focus of this article's analysis of the cyber security management model, which is based on managerial viewpoints.

Keywords: cyber security, management, critical infrastructure, cyber attacks

1. Introduction

Critical infrastructure is no exception to the rule that cyber security has surpassed all other concerns in today's globally linked environment. Critical infrastructure is defined in several ways. In an Executive Order (EO) dated 1996, the seven pillars of the United States' vital infrastructure were enumerated (Johnson, 2015). According to the EO, the electrical grid system, transportation, and telecommunications are the most crucial domains. In the event that any of these are damaged, the viability in comparison to every other essential system. In order to help organisations and businesses secure their vital infrastructure, this essay will primarily focus on the theoretical components of a cyber security management model.

The importance of cyber defences cannot be overstated in the modern day. In Lithuania, cyber security is defined as a collection of legal, information dissemination, organisational, and technical measures that are necessary to prevent, detect, analyse, and respond to cyber incidents. These incidents can be anything like: unauthorised access to communication and information systems (CIS), electronic communications networks or industrial process control systems; disruption or change to information systems (including management takeover); damage to, or destruction of, electronic information; withdrawal or restriction of access to, or use of, non-public information in electronic form. In the event of a cyber incident or cyber assault, the primary goal of the aforementioned measures is to facilitate the rapid restoration of electronic communications networks, information systems, and industrial process control systems.

The most critical goals for achieving cyber security may be determined using the recognised definitions of cyber security and cyber incidents. First and foremost, we want to make sure that no one other than authorised personnel may access, modify, or handle any data. The second goal is integrity, which makes sure that no one other than authorised processes may make modifications to the system. Thirdly, the accessibility of the system and the data that is under the control of the system's administrators. This goal guarantees that the organization's infrastructure will only allow authorised individuals to access the information and resources kept there. Cyber-security and management are inseparable and crucial parts of

every business, as any law-based regulation can attest. Cybersecurity is now considered just as crucial as physical security when it comes to protecting vital infrastructure (Ten, Manimaran, Liu, 2010).

A large number of academic institutions and private businesses have studied CIS security and security technologies. There have been several market-available security tools and technological standards aimed at bolstering CIS security, but a notable uptick in the last 20 years has been in the provision of universal security solutions for the protection of critical infrastructure.

The rapidly expanding reach of communication and information technology, the improvement in service delivery in terms of both convenience and efficiency (Limba et al., 2016), and the strengthening of energy infrastructure have all contributed to the maturation of the concept of cyber security in recent years (Wang, Lu, 2013). One may make the case that critical infrastructure vulnerabilities are likewise developing at a fast pace, which impacts system security.

System complexity and integration are major contributors to the growing number of potential points of failure. When smaller systems are integrated into larger ones, it raises the overall complexity of the system, which in turn makes it more likely that vulnerabilities will emerge in both domestic and international interconnected systems. The increasing demand for efficiency often drives the adoption of new modern technologies, but these advancements are seldom examined from a security perspective, particularly in cyberspace. This is because there is a lack of awareness of the specific areas where these technologies are most susceptible to attack, and there are currently no effective mechanisms in place to hold the private sector accountable for the harm they cause (Kroger, 2008).

Protecting vital infrastructure (such as online voting or banking systems) or vital energy infrastructure requires a cyber security management model, which is a consensus throughout all nations and scientific communities. Even though there isn't a universally accepted model for cyber security management, every nation understands the need of safeguarding its most valuable assets. Authorities and groups from

A nation's and its people's well-being can only be guarantyd if its vital infrastructure is secure, and this is particularly true in a time when energy and critical infrastructure security are being used as arguments in political decision-making (Tvaronavičienė, 2012). In 2000, the US government warned that cyber defences shouldn't be handled independently by individual states' information systems, but rather as part of a comprehensive national strategy (US GAO, 2007; Councel of Europe, 2008; NATO, 2010; Johnson, 2015).

Researchers from several nations have endeavoured to discover a cyber-security strategy that is both successful and efficient. They believe that it is of the utmost importance for countries throughout the world to work together to secure cyberspace for vital infrastructure. It should be emphasised that due to the interconnected nature of the critical infrastructure components, a cyber assault has the potential to cause extensive harm to other systems since a breach in one area may quickly propagate to another (Bulakh, 2016). Since the public sector often owns a portion of the vital infrastructure systems or communication networks that are often operated by private operators, it is necessary to enhance public-private partnerships in order to secure these resources. The European Commission is responsible for organising the critical infrastructure protection information distribution network, which is one of the public-private cooperation projects. Experts, representatives from the corporate sector, and public officials may all connect via this network to share knowledge and collaborate (European Commission).

The private sector, nevertheless, is noticeably less likely to provide details on individual assaults, even if doing so may greatly aid in the improvement of cybersecurity. Companies in the private sector are not likely to come clean about cyber assaults and infrastructure vulnerabilities, according to the European Commission and Rosner (2013). This is because doing so could damage their reputation and cause society and business partners to reconsider the attractiveness of working with them.

Ensuring the security of Supervisory Control and Data Acquisition (SCADA) systems, which are used to monitor and control features in the industrial sector and energy transit infrastructure, has received a lot of attention in cyber security studies. These solutions have been accepted in the cyber security protection field. There are four main components of SCADA system security: real-time monitoring, anomaly detection, impact analysis, and mitigation measures (Ten, Manimaran, Liu, 2010). In this situation, cyber security is examined only via a technical lens, which is not entirely accurate. While technological fixes to cyber security issues are crucial, a broader and more nuanced perspective on the cyber security paradigm is required in the modern day. It is advised that the business sector, national regulators, and governmental institutions all work together to build a cyber security model for the country's vital infrastructures. According to the US Department of Energy and the US Department of Homeland Security (2006) and the Organization for Security and Cooperation in Europe (2013), it is crucial to seek out the best international practices and regulations.

Because cyber security is more than just technology, the authors of this article will not focus on technical aspects of CIS security. Instead, they will attempt to present a theoretical model that can be utilised for cyber security management in order to secure critical infrastructure, as cyber security is both a part of and concurrent with critical infrastructure security (Fuschi, Tvaronavičienė, 2014).

2. Taxonomy of Critical Infrastructure Attacks

Cyber criminals Cybercriminals target essential infrastructure because they stand to gain politically or financially from an assault on this target. The most serious flaw is that the systems rely on commercial items, which means that an attacker with the right level of technical expertise may take advantage of security holes in those products the United States Department of Energy and the United States Department of Homeland Security (2006) on common operating systems and communications protocols. People have a lot of faith in the CIS and its technology, thus this is changing. Cyberattacks on vital industries can have far-reaching effects on both the public and commercial spheres. For instance, 225,000 people in Ukraine lost electricity in December 2015 due to an assault on the country's electrical grid. According to the US Department of Homeland Security, malicious software was used to carry out a cyber-attack. To the best of our knowledge, this is the first instance of a successful cyber breach that disrupted the power supply chain. There have been several efforts to identify the cyber-attack's origins, but the difficulty in determining who is responsible is inherent in every occurrence that takes place in cyberspace (Volz, 2016). The most effective way to stop cyberattacks is to make cyber security better. The likelihood that cyber assaults will be effectively executed is growing since cyber dangers are notoriously hard to foresee, forecast, and take appropriate precautions against.

Underestimating their susceptibility to cyber assaults and other unforeseen circumstances, many nations have not yet established a plan to counter them. Examining cyber-security concerns in the context of critical infrastructure is crucial for safeguarding key national interests. The cyber security management model of critical infrastructure has to be modified in tandem with the ever-changing technology, regulatory considerations, and other factors, since technical solutions alone cannot address all

issues (Limba, Agafonov, Damkus, 2016).

Critical infrastructure or industrial control systems (ICS) assaults are primarily focused on by government organisations (such as the US Department of Energy and US Department of Homeland Security) and researchers (such as Tranchita, Hadjsaid, Viziteu, Rozel, Caire, 2010). There are five main categories of attacks, which differ in terms of the goals the attacker has for the system:

Corruption of information – when data on a system or communications channel suffers improper modification.

- Denial-of-service (DoS) – when access to the system is denied for authorized users.
- Disclosure of information – when critical information is disclosed to unauthorized persons or systems.
- Theft of resources – when system resources are used by unauthorized entities.
- Physical destruction – when physical harm or destruction is achieved through the use of ICS.

US Department of energy and Department of Homeland Security also predicted that the cyber environment will change and therefore attack vectors to the critical infrastructure will change as well meaning owners and operators will need to combat new threats. The security posture of critical infrastructure will be increasingly challenged as technologies, business practices (Kiškis, Limba, Gulevičiutė, 2016), and market trends (Kiškis, Limba, 2016) continue to reshape the security landscape. Changes of technology (Vlasenko et al., 2016) will mean big changes in the field of system management and resistance to vulnerabilities.

Barnes and others identified that ICS cyber vulnerabilities originate from the point where connectivity is the greatest and access control is the weakest (Barnes, Johnson, Nickelson, 2004). They identify 4 domains of cyber vulnerabilities (each domain has its own attack vectors that are used by cyber criminals to achieve their goals):

- IT Domain.
- ICS Domain.
- Communications Domain.
- Physical Domain.

These days, it's impossible to keep the ICS and IT sectors apart. According to Marcelo, the most compelling reason for the integration of ICS and IT components in contemporary infrastructures, particularly electrical infrastructure, is the advancement and growth of technology (Marcelo, 2010).

According to the US Government Accountability Office, cybercriminal organisations are classified according to the objectives of the attackers: terrorists, phishers, insiders, bot-network operators, criminal organisations, foreign intelligence agencies, spammers, spies, and malware/spyware developers. While each of these organisations has its own unique motivations for attacking vital infrastructure or other IT assets, the fact remains that they are all very harmful (GAO, 2005).

To get control of the system they are targeting, attackers often attempt to exploit flaws and leverage several attack paths. The majority of the time, in order to accomplish their goals, attackers will research vulnerabilities (Stouffer, Falco, Kent, 2013). There are typically five steps to a cyber attack: identifying a system vulnerability, gaining control of the system or a portion of it, installing malicious software, infecting other parts of the system, and finally, attacking the whole system or parts of it. Figure 1 depicts each of these steps.

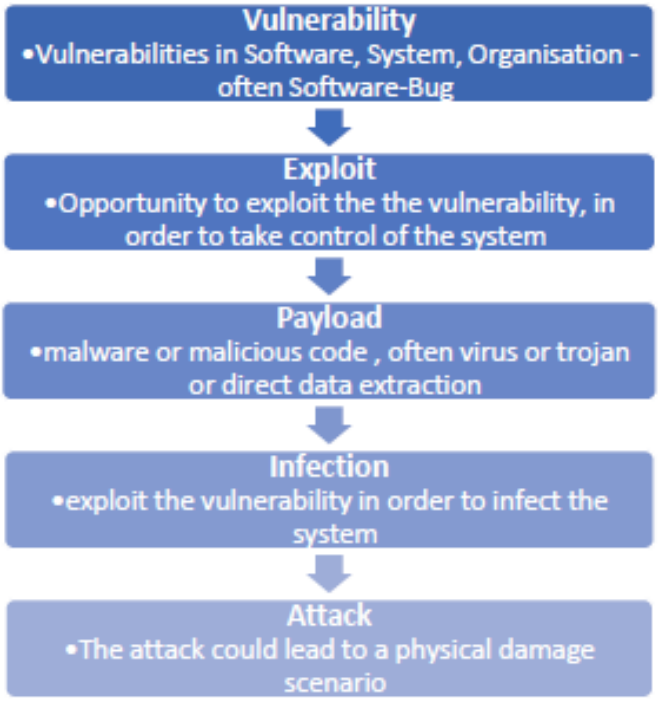

Fig. 1. Cyber attack development stages

Source: IMIA Working Group, 2016

Gaps in cyber security cause big issues to each system owner or operator, but they may not be perceived to be as critical as gaps in critical infrastructure systems, because the impact of attacking them will be mostly invisible. The attack on the system may have various impacts. Some attacks on critical infrastructures are described below. Whilst these are the most common attack types the reader must understand that this is not a finite list and the attackers can have other aims when attacking not just critical infrastructure:

- Some attacks on the infrastructure seek to cause panic in the population and disrupt usual life. The examples of these attacks are the Los Angeles traffic lights 2006 attack (GAO, 2007), Volgodonsk 2007 and St. Petersburg 2008 nuclear power plant attacks (Butrimas, Bruzga, 2012; sputniknews.com, 2008) and others.
- Espionage attacks like 2006/2013 US energy facilities attacks (Umbach, 2013), Red October 2012 (securelist.com, 2013), Gauss 2012 (kasperskylabs.com, 2012), Careto (the Mask) 2014 (kasperskylabs.com, 2014) and others.
- Attacks whose main aim is to destroy or disrupt the normal work of system equipment. F. e. 1982 USSR SCADA attack (Radziwill, 2015), 2000 Australian Sewage spill (Crawford, 2006), probably the most known nuclear power plant attack – STUXNET 2010 (Karnouskos, 2011; langner, 2013) and others.

Today we can't imagine the power supply backbone or other critical infrastructure without ICS control environment. The field of critical infrastructure management nowadays is impossible without modern technology, which simplifies and reduces operating costs but at the same time this technology has formed security gaps and created gates to exploit cyber vulnerabilities. The technology companies are trying to increase the resistance of the critical

energy infrastructure and eliminate cyber threats by creating a centralized system management model that protects critical infrastructure from cyber vulnerabilities, but sometimes new technologies just open new possibilities to attackers (Wei, Lu, Jafari, Skare, Rohde, 2010) and they will attack if the smallest chance is given.

3. Development of Cyber Security Management Model

The importance of this is that cyber threats are notoriously hard to foresee, anticipate, and counter in a timely manner (Craig, Valeriano, 2016), which means that cyber assaults are becoming more likely to succeed. Considering the present geopolitical climate, this is especially relevant to the situation in Lithuania. In order to protect the state's fundamental interests, it is crucial to address cyber security concerns within the framework of critical infrastructure, as no existing model for cyber security management enables a response to cyber assaults, unexpected scenarios, or vulnerabilities. While technology is always improving, it is important to remember that this does not mean that cyber security management models for critical infrastructure should rest on their laurels (Water Information Sharing and Analysis Center, 2015).

3.1. Cyber Security Mistakes

Many businesses make the following errors while planning for the cyber protection of their assets: • Assuming, incorrectly, that any vulnerability can be eliminated from any infrastructure. Full security is an ideal that no organization can achieve, and that includes those responsible for operating infrastructure, particularly vital infrastructure. Having a clear plan that outlines how to reduce losses and restore normal activity of your infrastructure is crucial for security. You must also know which areas are most vulnerable, what to do to avoid threats, and what mechanisms to use to detect abnormal activity (WISAC, 2015). Nevertheless, organisations should prioritise the identification and reaction to critical circumstances as a crucial part. According to Techrepublic (2004), these measures may greatly lessen the impact of cyber security breaches on financial losses. • Misinformation stating that you can protect yourself from cyber threats by hiring top talent. According to WISAC (2015) and Singer and Friedman (2014), cyber security is a strategy that every company should take. A false feeling of security is fostered when cyber security is recognised as a department and a professional association. This method is incorrect. Techrepublic (2004) and Wei, Lu, Jafari, Skare, Rohde (2010) both agree that the human element is the weakest link in cyber defences, so ensuring the safety of sensitive data should be an organization's top priority. So, for instance, the company's rules should include cyber security, which might affect profits. Some people have erroneous beliefs about security technology and tools. Technical equipment and software manufacturers will never provide a foolproof defence against cyber threats. Modern security features, such as the ability to detect an intruder, rely on technology and equipment. While these safeguards are essential and should be included in the IT infrastructure, remember that technology alone cannot provide complete protection from cyber threats (Techrepublic, 2004; Wei, Lu, Jafari, Skare, Rohde, 2010). Good and powerful cyber defence capacity must be in place before tools can be considered a finished product. However, IT departments aren't made of goods; rather, everyone must do their share to ensure cyber safety, and people are still the biggest vulnerability (WISAC, 2015). Only when individuals take ownership of their actions and try to secure their networks will investments in technologies be worthwhile. Take social engineering as an example; it remains a major threat to any business that prioritises its own security. This is an area where technology may be helpful, but ultimately, management must own up to the issue and find a solution. Businesses must realise that their employees, at all levels, need ongoing education on the dangers of cyber assaults. • The misconception that adequate monitoring is all that is required to ensure cyber security. The definition of "monitoring" here goes beyond the simple tracking of physical assets like machinery and buildings. The term "monitoring" refers to more than just keeping tabs on networks, data centers, and individual computers; it is a holistic approach that incorporates

environmental factors and the tracking of emerging patterns in cybercrime. Without the ability to draw conclusions, monitoring serves no use (WISAC, 2015). You may utilise what you know about external trends and developments in cyber security to design effective policies and plans that will help you win the battle against cybercrime. The foundation of every cyber security plan or policy should be lifelong education. In order to be ready for future risks, organisations must know how such threats will change and grow over time. In the long run, this method saves money compared to erecting ever-higher barriers, which only provide temporary protection. When it comes to security, it's everyone's responsibility to spread the word about any known vulnerabilities; otherwise, no one would have a complete view of the situation on a local, national, or global scale (Govindarasu, Hahn, 2017). • Misconceptions about the efficacy of the organization's security procedures in warding off cybercriminals. In order to accomplish its objectives, security must first be established. Like training for an Olympic marathon, creating strong cyber defences and attempting to thwart cyber assaults is an arduous and ultimately fruitless endeavour. As soon as an attacker comes up with a new strategy, the defences fall behind. Putting money into more advanced security systems to stave against assaults seems like a good idea, but the truth is a little different. Instead of funding cutting-edge systems and technologies that can identify any danger, the cyber security strategy should put a premium on investing in essential infrastructure and resources (WISAC, 2015). The first step is to identify the potential intruders and learn why they would be interested in the group's operations. As said earlier, immeasurable cost technologies can not guarantee perfect protection, thus it is important to know the worth of their assets in order to evaluate and take on some risk.
The most important thing about cyber security is that it shouldn't be forgotten till the project is over, but rather the foundation of new IT solutions and systems.

3.2. Dimensions of Cyber Security Management Model

Further on we will provide the cyber security management module which can be used to ensure security to any critical infrastructure as well as to improve the cyber security of any business company or government organization. However, we will not concentrate on usage of concrete technology equipment or information security management processes that are used for making critical infrastructure safer, but will provide core information about the proposed model. The whole model is presented in Fig. 2.

Fig. 2. Cyber security management model

Source: Designed by the authors

According to the authors, there are six main areas that must be considered while building a model to guarantee cyber security. The development of a single component of the model will not significantly impact the organization's security, hence it is necessary to work on all of these aspects simultaneously.

3.3. Levels of Cyber Security Model

Each dimension of the proposed cyber security management model can be divided in to 3 levels: *initial level, moderate level and full integration level*. *Initial level* of all dimensions is associated with the organizations ability to clearly identify which problems can be met by the organization during the implementation of the cyber security model:

This knowledge creates security and confidence inside an organization which can easily deal with cyber security threats and perhaps it is time to take a step toward the management model and finally understood that technology and management must walk hand in hand in order to ensure effective cyber security.

Conclusions

The existing There are typically two main parts to the current literature on cyber security, whether it be for critical energy infrastructure or other aspects of cyber defence. The first part is technical, and it focuses on discovering the best technical solutions; the second part is strategic, and it aims to find a model for cyber defence that meets the demands of responsive management and governance. It is important to remember that technological fixes alone will not make organisations, systems, or infrastructures more secure from cyber threats. Modern dangers are growing at a dizzying rate, therefore finding a solution that takes sophisticated steps is essential. The moment has come to formulate a model for cyber security management that takes into account all relevant strategic factors. Cybersecurity must be pushed to all sections of the company and every person of the organization must be active in cybersecurity, according to the cyber security management model given in this article. Additionally, it is essential that private sector organisations, public authorities, and the government all work together, despite the intricacy of their connections, to share worldwide best practices.

There are six components to the suggested approach for cyber security management. A company can lessen its exposure to cybercrime and its vulnerabilities, as well as learn about emerging trends in cybercrime and the kinds of attacks that could target it, by implementing the cyber security management model's four dimensions. The company will also be better able to communicate internally and with other companies, making it more resilient to cyberattacks and boosting its reputation.

There are three primary steps that a company may take to adopt the cyber security management model. You may get a different set of achievements at each level. It is possible to execute the suggested cyber security management model's first and second tiers (the initial and moderate level) independently. This implies that you may accomplish your objectives and make plans for progress in each dimension independently, without having to link them. To enter the integration level of the model, you must first achieve the second level for all model dimensions. At this tier, all aspects of the organization are fully interoperable, and everyone has a specific job. Reaching this stage does not imply that all measures have been taken, but rather that the organization is prepared to withstand any cyberattacks and can identify potential entry points. In today's linked world, the cyber security scenario is always evolving. Organisations must be prepared and recognise that cyber vulnerability protection strategies and technologies might become outdated. Because of this, companies must be flexible in their cyber security management strategies to accommodate future events that may not be part of their current plans.

References

In 2004, Barnes, Johnson, and Nickelson published a work. An overview of SCADA security and potential threats. Bulakh,

Tuohy, and Pernik (2016). Estonia's Developing Level Playing Field for Critical Energy Infrastructure Protectors - a Model for Broader Scale Platforms. http://dx.doi.org/10.2172/911209."Operational Highlights: Energy Security" (Volume 10, pages 4–10) is online at: https://www.icds.ee/fileadmin/media/icds.ee/failid/no 10/20160410.pdf.
Bruzga A. and Butrimas V. 2012. Per Concordiam: A Journal of European Security and Defence Issues Article on the Cybersecurity Aspect of Vital Energy Infrastructure The file can be accessed at this URL: http://www.marshallcenter.org/mcpublicweb/mcdocs/files/College/F_Publications/perConcordiam/pC_V3N4_en.pdf.

Carlton and Levy (2015) conducted an expert assessment of non-IT professionals' top platform independent cybersecurity skills. This information is sourced from the Council of Europe in 2008. An EU directive on vital infrastructures. The 2008/114/EC9 Council Directive. Easily accessible online: By Craig A. and Valeriano B. in 2016, this article was published in the European Union's official law journal. Article available online: Responding to Cyber Threats: Online Safety and Security in the Information Age, Global Security and Intelligence Studies 1(2). This sentence is paraphrased from an article in Computerworld Australia that discusses how a utility hack led to a security overhaul. It can be found online at: http://www.computerworld.com/article/2561484/security0/utility-hack-led-to-security-overhaul.html. The article is in reference to the Critical Infrastructure Warning Information Network, which is run by the European Commission. Easily accessible online: According to Fuschi and Tvaronavičienď (2014), the Critical Infrastructure Warning Information Network is located at http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/index_en.htm. Publicly available: Govindarasu M.; Hahn A. 2017. Cybersecurity of the Power Grid: A Growing Challenge. Journal of Security and Sustainability Issues 3(3): 5–14. Sustainable development, Big Data, and supervisory control: service quality in the banking industry. According to a recent article published on February 24, 2017, the power grid's cybersecurity is becoming an increasingly pressing issue.

The IMIA Group of Experts, 2016. Cyber Risks Engineering from the Viewpoint of Insurance Companies. IMIA Annual Conference, IMIA Working Group Paper 98 (16). Easily accessible online: By Jenab K. and Moslehpour S. in 2016, the following document was published: https://www.imia.com/wp-content/uploads/2016/09/IMIA-Working-Group-Paper-9816-Cyber-Risks-Rev-A002-16-09-20161.pdf. Cyber Security Management: A Review. The article is titled "Business Management Dynamics" and it is pages 16–39 long. The following document is accessible online: Johnson, T. A. 2015. Cybersecurity. http://bmdynamics.com/issue_pdf/bmd110587-%2016-39.pdf. Secure the Nation's Essential Services against Cyber Threats and Cyber Warfare. Released by CRC Press

Effects of the STUXNET Worm on the Safety of Cyber-Physical Systems in Industrial Organisations (Karnouskos, 2011). Conference of the IEEE Industrial Electronics Society, 39th Annual. 2014, Kasperski Lab, http://dx.doi.org/10.1109/IECON.2011.6120048. "The Mask" is one of the most sophisticated global cyber-espionage operations ever discovered, according to Kaspersky Lab, thanks to the sophisticated toolkit used by the attackers: Unveiling the Mask (v1.0.pdf) by Kasperski Lab, 2012, available at https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/. The Kaspersky Lab has uncovered a new and sophisticated cyber-threat called "Gauss" that targets online banking accounts: Here is the link to the press release: http://newsroom.kaspersky.eu/fileadmin/user_upload/en/Images/Lifestyle/Kaspersky_Lab _Press_Release_Gauss_-09.08.2012.pdf. I

Biotechnology patenting in developing nations: approaches for the global market (Kiškis M.; Limba T. 2016). This is the Biotechnology Law Report, volume 35, issue 6, pages 291-299. In 2016, Kiškis, Limba, and Gulevičiūtė published a work with the DOI number 10.1089/blr.2016.29035.mk. Case Studies of Lithuanian and Arizonan (US) Firms on the Business Value of Intellectual Property in Biotech SMEs. Sustainable Business Practices and Entrepreneurship 4(2): 221-234. URL: http://dx.doi.org/10.9770/jesi.2016.4.2(11) Kroger WW. 2008. Important infrastructures under jeopardy: A need for fresh thinking and more comprehensive analysis, Reliability Engineering & System Safety 93(12): 1781-1787. Reference: Langner R. 2013, http://dx.doi.org/10.1016/j.ress.2008.03.005. An Online Technical Analysis of the Goals of Stuxnet's Developers: "To Kill a Centrifuge" The sentence might be paraphrased as: "Law firm Langner has a strategy to kill centrifuges" on Lithuania's National Cyber Defence. Easily accessible online: Visit https://www.e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4 for information.

Presented at the 16th International Interdisciplinary Conference on Social Innovations in September 2016 in Vilnius, Lithuania, this paper by Limba, Agafonov, and Damkus examines cyber security from a managerial perspective, drawing on both theoretical and practical insights.

In 2016, the authors Limba, Gulevičiūtė, Kiškis, and Romeika published a joint work. Use of E-Business Qualitative Criteria in International Market Research. Business and Economics: Revolutions, Pages 645–659.

The National Security Strategy of Lithuania. Online at: https://www.e-tar.lt/portal/lt/legalAct/TAR.FD615B2F7F90.

In 2010, Lukszo, Z., Deconinck, G., and Weijnen, M. P. C. The Importance of Cybersecurity for Electricity Supply. Macaulay T. (2008) was published by Springer. Knowing the Interdependencies, Parts, Vulnerabilities, and Operating Risks of Critical Infrastructure. Released by CRC Press

According to Masero (2010). Power Infrastructure Information and Communication Technology Security: A Governance Perspective. The North Atlantic Treaty Organization (NATO) published this in 2010. The North Atlantic Treaty Organization's members' defence and security are outlined in the following

document: Active Engagement, Modern Defence, and the NATO Summit in Lisbon Adopted Strategic Concept for Defence and Security. Easily accessible online: 68580.1.html is the URL for the official texts section of NATO's website.