The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 4 Number 4 (June)
http://doi.org/10.9770/jesi.2017.4.4(12)

Publisher

CYBER SECURITY MANAGEMENT MODEL FOR CRITICAL INFRASTRUCTURE

Tadas Limba[1], Tomas Plėta[2], Konstantin Agafonov[3], Martynas Damkus[4]

[1,3,4] Mykolas Romeris University, Ateities g. 20, 08303 Vilnius, Lithuania

[2]NATO Energy security center of excellence, Šilo g. 5a, 10322 Vilnius, Lithuania

E-mails:[1]tlimba@mruni.eu; [2]tomas.pleta@enseccoe.org; [3]ka1979@gmail.com; [4]martynas.damkus@gmail.com

Received 18 February 2017; accepted 20 April 2017 .

Abstract. Cyber security is the most critical aspect nowadays of our technologically based lives. Government institutions, banking sectors, public and private services, nuclear power plants, power grid operators, water suppliers or waste water treatment companies use information technologies in their day-to-day operations. Everything that uses technologies are based on communication and information systems and that means that it depends on cyber security. The public and private sector each year spend millions of dollars on technologies, security software and hardware devices that will increase the cyber security inside their companies, but they are still vulnerable. The main problem of this situation is that cyber security is still usually treated as a technical aspect or technology which can be easily implemented inside the organization and this implementation will guarantee cyber security. This attitude must change, because cyber security nowadays is something more than just the technology. This article presents the taxonomy of the critical infrastructure attacks, analyzes attack vectors and attack methods used to damage critical infrastructure as well as the most common cyber security mistakes which organizations make in the cyber security field when trying to make themselves safer from vulnerabilities. The main aim of this article is to provide theoretical aspects of the cyber security management model which can be used to ensure security of critical infrastructure in an organization or company. The cyber security management model that is presented in this article is analyzed from management perspectives and is not concerned with technological aspects and products that are used to protect critical infrastructure from cyber security attacks and vulnerabilities.

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

Reference to this paper should be made as follows: Limba T.; Plėta T.; Agafonov K.; Damkus M. 2017. Cyber security management model for critical infrastructure, *Entrepreneurship and Sustainability Issues* 4(4): 559-573. http://dx.doi.org/10.9770/jesi.2017.4.4(12)

JEL Classifications: D80; M15; O33

Additional disciplines: Information and Communication; Energetics and Thermoenergetics; Informatics

1. Introduction

Nowadays in our interconnected world cyber security has become the most important thing that influences every part of our life, especially regarding critical infrastructure. There are a lot of definitions of critical infrastructure. In 1996 The President of the United States issued an Executive Order (EO) which listed seven areas of critical infrastructure of the US (Johnson, 2015). The EO also stated that the most important areas are: the system of electrical grids, transportation and telecommunications. Damage to any of these will have impact on the viability

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 4 Number 4 (June)
http://doi.org/10.9770/jesi.2017.4.4(12)

of all other critical infrastructure. The main aim of this article is to provide theoretical aspects of the cyber security management model which can be used to ensure security of critical infrastructure in an organization or company.

It should be emphasized that cyber security nowadays is not just a technical issue. Lithuanian Cybersecurity law defines cyber security as a set of legal, information dissemination, organizational and technical measures which are needed to be taken to prevent, detect, analyze and respond to cyber incidents, which are described as the event or activity that causes or may cause or allow: unauthorized access to communication and information systems (CIS), electronic communications networks or industrial process control systems; can disrupt or change information systems, including the management takeover; electronic communications networks or industrial process control operations to destroy, damage, delete or modify electronic information, withdraw or restrict access to electronic information, as well as enable to absorb or otherwise use non-public information in electronic format by unauthorized persons (Law on Cyber Security of the Republic of Lithuania, 2014). The main purpose of the mentioned actions is to provide fast recovery of electronic communications networks, information systems or industrial process control system in case of cyber incidents or cyber attacks.

Based on the approved cyber security and cyber incident definitions, it is possible to identify the most important objectives in order to ensure cyber security. The first objective is confidentiality which ensures that only authorized individuals can receive, change or manage information. The second objective is integrity, which ensures that only authorized persons or processes are able to carry any changes in the system. Thirdly – the availability of system and information which is managed by the system and its operators. This objective ensures that only authorized entities will have access to the information or resources stored or used in the organizations infrastructure. Law-based regulation clearly indicates that cyber-security and management are closely related and very important aspects of each organization. In order to ensure the security of critical infrastructure, it is recognized that cyber security is as important as the physical security (Ten, Manimaran, Liu, 2010).

CIS security and security tools were analyzed by a lot of commercial companies and scientists. A lot of security tools and technical standards were provided to the market to improve the security of CIS, but in last two decades there has been a significant interest in providing universal security tools to critical infrastructure protection.

Nowadays the meaning of cyber security is maturing, because of the rapid spread of communication and information technology to all parts of our life, more convenient and more efficient service delivery (Limba et al., 2016) as well as the increase in the energy infrastructure integrity (Wang, Lu, 2013). It can be argued that the vulnerabilities in critical infrastructure are also maturing rapidly and this process influences the security of systems.

The main problem of the increasing vulnerability can be associated with the complexity of the system and integration process: the small elements of the systems or small systems are integrated into larger systems which increases the system complexity and creates conditions for vulnerabilities to arise not only in domestic but also in countries interconnected systems; new modern technology usage is usually motivated by the increasing need for efficiency, but it is not considered from the security and especially cyber security position due to a lack of proper understanding of the vulnerable areas and limitations as well as a lack of possibilities to enforce the responsibility of private sector players to reduce the effect of their negligence on society or some part of society (Kroger, 2008).

One thing that each country and each scientist agrees on is that a cyber security management model is necessary if you want to secure your critical infrastructure (e.g. internet voting systems or banking systems) or critical energy infrastructure. However, although there is no single cyber security management model, all countries of the world are aware of the need to carefully manage and protect their critical resources. Governments and organizations of

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 4 Number 4 (June)
http://doi.org/10.9770/jesi.2017.4.4(12)

the world understand that the main efforts should be taken to provide security for their critical infrastructure because only this can ensure the wellbeing of the country and its people, especially when critical infrastructure and energy security has become an argument for political decisions making (Tvaronavičienė, 2012). The United States already pointed out in 2000 that cyber security must be managed holistically, rather than in separate state information systems (US GAO, 2007; Councel of Europe, 2008; NATO, 2010; Lithuania National Security Strategy, 2012; Johnson, 2015).

Researchers from different countries have attempted to look for an effective cyber-security model. In their view, ensuring cooperation on critical infrastructure cyber security is crucial both at domestic and international level. It is noted that since the critical infrastructure elements are very closely linked, a cyber attack can spread very widely and damage other systems as a breach in one area can easily spread to the other (Bulakh, 2016). It is essential to strengthen public-private partnerships in securing critical infrastructure resources, usually because the public sector is the owner of some part of the critical infrastructure systems or communication systems which is usually managed by private operators. It should be noted that one of the public - private partnership initiatives is organized by the European Commission – they have created the critical infrastructure protection information dissemination network. This network allows the public authorities, private sector representatives and experts to exchange and share information and best practices (European Comission).

However, it is noted that the private sector is much less inclined to share information about specific attacks even though such information could significantly contribute to the strengthening of cybersecurity. It is assumed that it is unlikely for the private sector to share the information about cyber security attacks and vulnerabilities they have identified in their infrastructure because this information can ruin their reputation and make society or business partners rethink the attarctiveness of collaboration (European Comission; Rosner, 2013).

Many cyber security studies have been focused on technical solutions which can be accepted in the cyber security protection field: much attention is given to ensuring the security of Supervisory Control and Data Acquisition (SCADA) systems that are used to monitor and control features in the industrial sector and energy transit infrastructure. The security of the SCADA system consists of four major elements: real-time monitoring, detection of anomalies, impact analysis and mitigation strategies (Ten, Manimaran, Liu, 2010). Cyber security in this case is analyzed only from a technological aspect, but this view is not fully correct. Technological solutions to strengthen cyber security are very important but, in reality, today you need a wider and more nuaunced view regarding the cyber security model.

When developing the country's critical infrastructures cyber security model it is also recommended to involve public institutions, national regulators and the private sector. It is important to look for the most effective regulation and international practices (US Department of energy, US Department of Homeland Security, 2006; Organization for Security and Cooperation in Europe, 2013).

The authors of this article will not concentrate on CIS security technology aspects, because as ha been mentioned earlier, cyber security is not just technological, authors will try to provide a theoretical model that can be used for cyber security management to also secure critical infrastructure because cyber security is concurrent with critical infrastructure security and is the main part of it (Fuschi, Tvaronavičienė, 2014).

2. Taxonomy of Critical Infrastructure Attacks

Cyber criminals concentrate their attention on critical infrastructure because in case of a successful attack you can get financial or political profit. The biggest vulnerability of this situation is that the systems use commercial products and with some technical knowledge the attacker can exploit vulnerabilities that exist in those products,

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 4 Number 4 (June)
http://doi.org/10.9770/jesi.2017.4.4(12)

telecommunication methods, and common operating systems (US Department of energy, US Department of Homeland Security, 2006).

This situation evolves because of deep trust in the CIS and technologies. Cyber-attacks on critical sectors usually have a big influence to the government and private sector. As an example, in December 2015 an attack on the Ukrainian power supply system cut off 225,000 users. The US Department of Homeland Security stated that a cyber-attack was executed through malicious software. This incident is probably the first known incident that was a successful cyber intrusion in interrupting the power supply chain. There have been a lot of attempts to find the initiators of the cyber-attack, but with incidents in cyber-space, you are always faced with the problem of attributing responsibility – it is extremely difficult to trace the perpetrators of the incident (Volz, 2016). In order to prevent cyber-incidents, the best response is the improvement of cyber security. It is important to note that cyber threats are particularly difficult to predict, anticipate and take timely preventive measures, so the risk that cyber attacks will be successfully implemented is increasing.

A lot of countries have not developed a strategy on how to respond to cyber attacks and unexpected scenarios and underestimate their vulnerabilities. It is extremely important and relevant to exam cyber-security aspects in a critical infrastructure context in order to ensure protection of vital national interests. It should be noted that the mere technological solutions do not solve all the problems and the cyber security management model of critical infrastructure should be improved along with the rapidly evolving technology, legal aspects and etc. (Limba, Agafonov, Damkus, 2016).

Government organizations (US Department of energy, US Department of Homeland Security) and researchers (Tranchita, Hadjsaid, Viziteu, Rozel, Caire, 2010) make attention to the main type of attacks on critical infrastructure or industrial control systems (ICS). Attacks can be described by five major groups which vary according to the objectives pursued by the attacker of 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.

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 4 Number 4 (June)
http://doi.org/10.9770/jesi.2017.4.4(12)

Nowadays the ICS and IT domains can't be separated. Marcelo indicates that modern infrastructures, and especially power infrastructure, integrate ICS components with IT components and the biggest argument for this situation is technological evolution and progress (Marcelo, 2010).

US Government Accountability Office identify cyber attacker groups by the goals that the attacker is trying to reach by his activity: Bot-network operators, Criminal groups, Foreign intelligence services, Hackers, Insiders, Phishers, Spammers, Spyware/malware authors, Terrorists. All these groups are targeting critical infrastructure or other information technology assets for the different purposes, but all of them are really dangerous and any group can be identified as innocuous (GAO, 2005).

Each attacker usually will try to exploit system vulnerabilities and use a few attack vectors to take the control of the system that he is trying to damage or exploit. In most cases attackers will study vulnerabilities in order to achieve their objectives (Stouffer, Falco, Kent, 2013). A cyber attack frequently develops in five different stages: finding a vulnerability of the system, taking control of the system or part of it, inserting malicious software into the system, infecting other system components and making an attack to all of the system or to special part of it. All these stages are shown in Fig. 1.

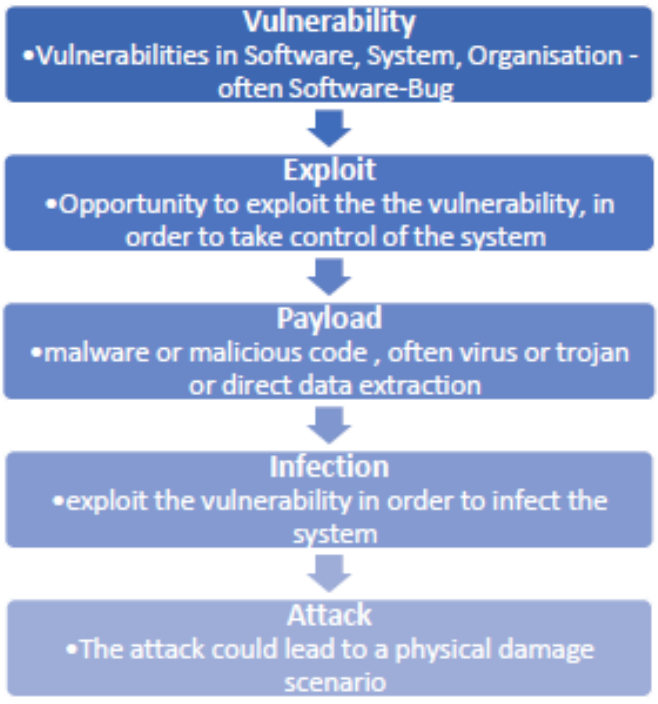

Fig. 1. Cyber attack development stages

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 International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 4 Number 4 (June)
http://doi.org/10.9770/jesi.2017.4.4(12)

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

What is important is that cyber threats are very difficult to predict, anticipate and take preventive measures in time (Craig, Valeriano, 2016), so the risk that cyber attacks will be successfully implemented is increasing. This is particularly true in the case of Lithuania, especially in view of the current geopolitical situation. Currently there is no cyber security management model developed which allows a response to cyber attacks, unexpected scenarios and vulnerabilities, so it is vitally important to deal with cyber security issues in the context of critical infrastructure, in order to safeguard the basic interests of the state. It should be noted that the mere technological issues and solutions do not solve all the problems as a cyber security management model of critical infrastructure should be constantly improved along with the rapidly evolving technology (Water Information Sharing and Analysis Center, 2015).

3.1. Cyber Security Mistakes

There are common mistakes that organizations make when thinking about the cyber security of their assets:

- Falsly thinking that each infrastructure can be made safe from any vulnerability. Each organization that operates infrastructure and especially critical infrastructure should understand that full security is just a dream. The most important aspect of security is to understand what are the most vulnerable areas, what activities you must do to avoid threats, which mechanisms you need to detect abnormal infrastructure activity and have a clear plan which describes how to reduce losses and to restore normal activity of your infrastructure (WISAC, 2015). However, a fundamental aspect which should be the most important to organizations is the *detection* and *response* for critical situations. These things can significantly reduce loses concerned with cyber security breaches (Techrepublic, 2004).
- False opinions that recruiting the best professionals will save you from the cyber threat. Each organization needs to understand that cyber security is not a department but a whole organization's approach (WISAC, 2015; Singer, Friedman, 2014). Qualifying cyber security as one of the department and professional

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 4 Number 4 (June)
http://doi.org/10.9770/jesi.2017.4.4(12)

association form deceptive sense of invulnerability. This approach is flawed. Cyber security must be a fundamental objective and must become a key aim of each organization's team member, because the human factor is the most vulnerable part in cyber security (Techrepublic, 2004; Wei, Lu, Jafari, Skare, Rohde, 2010). This means that, for example, cyber security should become one of the organization's policies, which can influence earnings.

- False thinking about security technologies and tools that are used to ensure the security. Companies that produce technical equipment and software will never guarantee that their products will defend you from 100 percent of cyber attacks. Technology and equipment used in the modern world to the fulfillment of certain security features such as detecting an intruder or etc. These measures and tools are very important and must be used in the technological infrastructure, but it is just technology and it can't grant you total cyber security (Techrepublic, 2004; Wei, Lu, Jafari, Skare, Rohde, 2010). Tools have to be a certain product, which occurs after the time when good and strong cyber defense capability is deployed. But products alone don't make the IT department, everyone is responsible for cyber security and the human factor remains the weakest link in relation to security (WISAC, 2015). Investment in tools is meaningful only when people are aware of their personal responsibility and seek to keep their networks safe. As an example: social engineering, which is still one of the main risks facing an organization taking care of their own security. Technology can help in this regard, but it is very important that managers take responsibility in solving this problem. Organizations need to understand that each person in the company needs to be evolved in education and must understand the threat of cyber attacks.
- False opinion that cyber security is just about effective monitoring. Monitoring in this context has a more broad meaning than just monitoring of equipment and infrastructure assets. Monitoring is not a narrow technical view, which is linked to specific information resources, information systems and network monitoring, but is a broad view, which combines in itself the whole organization of the surrounding environment and modern cybercrime trends tracking. Monitoring is worthless if no one can learn from it (WISAC, 2015). If you understand the external changes and trends in the cyber security you will be able to use these insights, and develop appropriate policies and strategies to be successful in the fight against cybercrime in the long run. Cyber security policy and strategy must be based on continuous learning and development. Organizations need to understand how threats evolve and develop in the future, and what the opportunities to prepare for the upcoming threats are. This approach is ultimately more cost effective because they have certain advantages over a short-term increase in security by building higher and higher walls. Each organization must ensure that the information about the security vulnerability is shared to others, because only the exchange of information may provide a general picture of the actual security situation in the city, state or the world scale (Govindarasu, Hahn, 2017).
- False opinions that security measures that are used by the organization to protect itself from cyber threats are superior. Security should first be determined to achieve its goals. Making effective cyber security and trying to avoid cyber attacks is like running in Olympic marathon, but security is not winning vs. cyber attackers. The attackers develop new methods and techniques, and defenders are always one step behind. It seems that it is useful to invest in increasingly sophisticated security measures to prevent attacks, but the reality is somewhat different. The cyber security policy must prioritize investment in critical infrastructure and resources, rather than the latest technology or systems that can detect any threat (WISAC, 2015). First of all, you need to understand what kind of invaders could be interested in the organization's activities and why. We must understand the value of their assets, to be able to assess and assume some risk because immeasurable cost technologies, as has been said before, do not ensure complete security.

The main aspect of cyber security is that cyber security should be the cornerstone of the development of new IT solutions and systems, and not, as often happens, remembered only at the end of the project like has happened

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 4 Number 4 (June)
http://doi.org/10.9770/jesi.2017.4.4(12)

with the internet architecture which was designed to promote connectivity, not security (Jenab, Moslehpour, 2016).

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

The presented model is constructed from the six core fields that the authors find to be most critical in the process of ensuring cyber security. All these elements have thesame importance and need to be developed thorughout the whole organization all together, because just the development of the one part of the model will not make any big changes to the security in organization.

As it was shown in the earlier figure, the model consists from the six core sections:

1. Legal regulation. This part of the model is constructed from requirements and legal proceedings and aspects that need to be achieved by the organization which is thinking about the modern cyber security. It must contain the whole vision of all legislation acts which will be used in organizations

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 4 Number 4 (June)
http://doi.org/10.9770/jesi.2017.4.4(12)

each day life (security instructions for employees, information security officers and network administrators, any standards which are used or are planned to develop in organization and etc.);

2. Good governance. In terms of cyber security achievement, this is maybe the most important part of the cyber security management model. Each modern organizational leader needs to understand the main aims of cyber security in their organization and understand that there are risks that will be never excluded from organizational life. The organization needs to understand that you can't do anything to avoid all cyber risks, but you can minimize the impact of cyber incidents to the organization if they occur. Cyber security must be the first stone in any project pedestal. Any project or activity which is planned within the organization must first be fully reviewed from a security perspective. Only a good understanding that security, and especially cyber security, is the core element of any project will provide success to organization projects and will help to save money and resources.
3. Risk management. This is the organizations ability to properly identify risks that are growing around the organization and ensuring they have the specialist skills to control the impact of these risks. As was mentioned earlier, organizations can't avoid all risks.Sometimes it is more important to have all risks identified and have a contingency plan than try to avoid all risks. In fact, the organization must learn not only to avoid risks, but also learn to accept them. Sometimes the ability to identify the risks and prepare contingency plans will do more for the organization than attempting to avoid the identified risks. Only after careful consideration of all risks can the question be answered; what is more effective, avoidance or the use or counter-measures?
4. Security culture. This needs to be integrated in the cyber security management model. This dimension is probably the hardest to implement and control. You can use informatics, mathematics or risk management technologies to attempt to calculate what is more beneficial to organization – buying new security system or accepting the risks of theft, but it is much more difficult to with your personnel, because they are people. This aspect is very important and the organization needs to understand that it is vulnerable as the people who are working there. Security must be understandable for every organization member and each member must have an ability to learn how to defend the organization and themselves from cyber security incidents as mistakes can be critical to the security of the organization. One of the biggest cyber security mistakes in this dimension is usually associated with the opinion of higher managers and IT specialists that they must have more privileges and access on their systems. If you need really to be protected and want to have fewer troubles with cyber security, you need to understand that all security measures must be available to all personnel personnel; otherwise you can lose your struggle for cyber security.
5. Technology management. As has been mentioned before, cyber security is not just about the technological approach to the organization but you will need to use it to achieve your organizational goals. Try to understand that your knowledge about each component that is controlled by IT can be vulnerable. You will need to know each component that you use for your organization work. This knowledge will let you know if there are some components which are vulnerable and can be the breached. The management of technologies and components will let you decrease the time which is needed to remove the effects of the security incident or prevent the rise of security incident.
6. Incident management. This dimension is closely attached to legal dimension of the module. You must have special plans regarding the incident consequence management. These plans need to include instructions to organization members which must be applied if any secure incident happens. You need to identify which measures must be implemented when trying to reduce the impact of the incident and how to restore normal operation to your organization.

Each field (dimension) of the proposed cyber security management model must be clearly identified, measured and evaluated and the organization needs to develop a clear plan regarding the problems that are identified in each field of the cyber security management model.

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 4 Number 4 (June)
http://doi.org/10.9770/jesi.2017.4.4(12)

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:

- The legal dimension will consist of the deep analysis of the legal framework inside and outside the organization and identification of all the gaps in the legal aspects that can affect the cyber security policies of organization;
- The good governance dimension will include the analysis of the governance system in the organization, with the possibility to identify which department or individual is involved in to the decision making process. Even a small understanding of the governance process in the organization and the governance process cooperation with the cyber security field will make the organization a little bit stronger on cyber security arena;
- The risk management dimension initial level collates all the risks that have any possibility to appear inside or outside the organization and can affect the organizations normal life and operation;
- The security culture dimension needs the clear understanding of the organization and its members about all security measures which can be used inside the organization to try to increase cyber security;
- The technology management dimension must include a clear vision of the all technologies used in the organization on daily working processes. Only a clear view of existing technologies that are used in the organizational life can identify what can be used as attack vectors to these technologies and what measures can be used to prevent or minimize attacks;
- The incident management dimension initial level in the organization must contain the organizational ability to understand that each organization can be damaged through technological or social aspects and this damage can appear at any time from any infrastructure segment (hardware or software) or personnel. Incident management on this level can contain simple instructions to the organization that can be used in the case of abnormal activity against the organization. The understanding of the cyber incident nature is the first, and maybe the main, step to increasing cyber security in the organization.

Moderate level of each of the six cyber security management model dimensions includes the clear plan and visibility of changes, which need to be done in organization:

- The legal aspects need to be clearly identified and all working instructions need to be prepared and introduced to each member of the organization
- The good governance dimension needs to clearly identify the governance chain in the organization with clear borders of responsibility for each department that is involved in organizational life;
- The risk management dimension needs to identify the clear plan of avoiding or accepting the risks which were identified in the initial level of the cyber security management model, because sometimes the better decision is to accept some risks than try to avoid them (it costs more or takes huge resources);
- The security culture dimension in the moderate level needs to include a clear plan of managing the personnel and providing a clear identification of skills that need to be reached by each organization member (you need to plan additional training for your IT security specialists and IT system users because only qualified IT personal should not be the warranty of your cyber security);
- The technology management must include clear and understandable information about the software and technologies that are used in the organization, including the life cycle of used equipment and

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 4 Number 4 (June)
http://doi.org/10.9770/jesi.2017.4.4(12)

software, because most security breaches are hiden inside the systems that are outdated, but still used in organizational working process (this technology audit needs to be done continuously, because it will let you plan financially what upgrades are needed for your existing equipment);

- The incident management dimension in this level needs to contain detailed plans and directions about the organizations recovery plans if any cyber security incidents occure and the normal work of the organization is disrupted. Each department of the organization or organizational member needs to know the disaster recovery plan if a cyber security attack on the organisation is susccessful.

The moderate level of each dimension in the cyber security management model is like the well trained soldier who has enough knowledge how to accomplish his mission, but doesn't forget that even well trained soldiers sometimes need training to refresh his knowledge. Organizations need to do timely audits of the cyber security management model dimensions and timely updates to all plans. Organizations need to remember that the world is changed by the computer technologies and this change process is still happening. When organizations try to survive in the real world they need to adapt to the changes and play by the rules of todays technologies and technologies that will appear in the future. Otherwise the modern organization will struggle to survive in our interconnected world and each organization needs to understand that it is impossible to create its own Arthur Conan Doyle's Lost world.

The highest level of the cyber security management model is the *full integration* (interoperability) level. It is defined by the full interconnection of all management model dimensions. On this level the organization is operating like a large army of soldiers working on one general mission and each dimension of the cyber security model is an inherent part of the organization.

The integration of the cyber security management model into the organization is a very difficult process which requires substantial understanding, and this knowledge can't be associated with the technology or information security fields. The biggest issue is to link technologies and management together, because often technical and management specialist talk different languages. Your organization will change when you begin to understand cyber security not as a technological discipline but as a real management challenge.

The model which has been presented in this article confers some advantages to organizations which implement it. All the dimensions of the presented model need to be auditable and renewed on a timely basis and this process will give the organization a better understanding of the cybercrime world around it and information about cyber security trends that help the organization make the right decisions and be more resistant to the cyber attacks. It also confers the ability to enable organizational leaders to actively participate in decision making and shaping the cyber security policy as well as an opportunity to properly assess the risks related to security and proper identification of such risks. The ability to learn how to manage incidents and reduce the effects of a successful attack helps all members of the organization understand cyber security threats by knowing what actions need to be done to reduce the ongoing attack symptoms or which actions need to be taken to avoid vulnerabilities. The ability to improve the organisations reputation in the outside environment because the organization really cares about cyber security is more attractive to consumers or business partners including the ability to moderate communication inside the organization, which helps to make organization more resistant to attack.

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

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 4 Number 4 (June)
http://doi.org/10.9770/jesi.2017.4.4(12)

The existing literature, which deals with critical energy infrastructure cyber security as well as with cyber security in other dimensions usually consists of two main sections: first, technical analysis, including finding the most effective technical solutions, whilst the second strategic-level analysis attempts to find an effective model for cyber security, ensuring the needs of responsive governance and management. It should be noted that the technical solutions is not the panacea that can improve cyber security for organizations, systems or infrastructures. Nowadays when the threats are increasing rapidly, you need to think about the solutions that have more complex measures. It is time to think about a cyber security management model which has considered all strategic aspects. The main idea of the cyber security management model that has been presented in this article is that cyber security must be pushed to all parts of the organization and each member of the organization must be involved in cyber security. Also it must include the involvement of government, public authorities and private sector organizations cooperating and sharing international best practices, despite the complexity of their interactions.

The proposed cyber security management model includes six dimensions. The implementation of the cyber security management model dimensions in an organization will help to minimize the risks and limit the impact of successful cyber attacks which can be initiated against the organizations infrastructure, have a better understanding of the security situation around the organization and inside it (this will provide necessary knowledge about the vulnerabilities of the organization, cybercrime trends and attacks that could be executed against the organization), provide better communication inside the organizationas well as improving the communication with other organizations which makes them more resistant to attacks and improves the organizations reputation.

The implementation of the cyber security management model in an organization could be made by three initial levels. Each level has its own line of achievement. The first and second levels (initial and moderate level) of all dimensions in the proposed cyber security management model can be implemented separately. This means that you can achieve the goals and prepare improvement plans of each dimension separately and these plans need not be connected together. Only after the second level is reached for all dimensions of the model can you step into the *integration* level of the model. This level has full interoperability through all dimensions and each member of the organization has their own role. The achievement of this level means that an organization is able to resist cyber attacks that can be attempted against it and can predict the main attack vectors, but it doesn't mean that everything is done. The cyber security situation in todays interconnected world is changing second by second and organisations need to be prepared and understand that plans that are prepared today and that technology that is used to protect you from cyber vulnerabilities can be rendered obsolete tomorrow. This means that the cyber security management process is very dynamic and organisations need to be prepared for situations that are not in their plans and that need to be covered in the future.

References

Barnes K.; Johnson B.; Nickelson R. 2004. *Introduction to SCADA protection and vulnerabilities.* http://dx.doi.org/10.2172/911209

Bulakh A.; Tuohy E.; Pernik P. 2016. Estonia's Developing Level Playing Field for Critical Energy Infrastructure Protectors - a Model for Broader Scale Platforms?, *Energy Security: Operational Highlights* 10: 4-10. Available on the Internet: https://www.icds.ee/fileadmin/media/icds.ee/failid/no_10_20160410.pdf

Butrimas V.; Bruzga A. 2012. The Cyber Security Dimension of Critical Energy Infrastructure, Per Concordiam, *Journal of European Security and Defense Issues*, Available on the Internet: http://www.marshallcenter.org/mcpublicweb/mcdocs/files/College/F_Publications/perConcordiam/pC_V3N4_en.pdf

Carlton M.; Levy Y. 2015. Expert Assessment of the Top Platform Independent Cybersecurity Skills of Non-IT Professionals, 2015. http://dx.doi.org/10.1109/SECON.2015.7132932

Council of Europe, 2008. The European Critical Infrastructures Directive. Council Directive 2008/114/EC9. Available on the Internet: http://eur-lex.europa.eu/legal-content/DA/ALL/?uri=CELEX:32008L0114

Craig A.; Valeriano B. 2016. Reacting to Cyber Threats: Protection and Security in the Digital Age, *Global Security and Intelligence Studies* 1(2), Available on the Internet: http://digitalcommons.apus.edu/gsis/vol1/iss2/4

Crawford M. 2006. Utility hack led to security overhaul, *Computerworld Australia*, Available on the Internet: http://www.computerworld.com/article/2561484/security0/utility-hack-led-to-security-overhaul.html

European Commission, Critical Infrastructure Warning Information Network. Available on the Internet: http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/critical_infrastructure_warning_information_network/index_en.htm

Fuschi, D.; Tvaronavičienė, M. 2014. Sustainable development, Big Data and supervisory control: service quality in banking sector, *Journal of Security and Sustainability Issues* 3(3): 5-14. http://dx.doi.org/10.9770

Govindarasu M.; Hahn A. 2017. *Cybersecurity of the Power Grid: A Growing Challenge*, Available on the Internet: https://www.usnews.com/news/national-news/articles/2017-02-24/cybersecurity-of-the-power-grid-a-growing-challenge

IMIA Working Group, 2016. Cyber Risks Engineering Insurers Perspective. *IMIA Working Group Paper* 98 (16), IMIA Annual Conference. Available on the Internet: https://www.imia.com/wp-content/uploads/2016/09/IMIA-Working-Group-Paper-9816-Cyber-Risks-Rev-A002-16-09-20161.pdf

Jenab K.; Moslehpour S. 2016. Cyber Security Management: A Review. *Business Management Dynamics* 5(11): 16-39. Available on the Internet: http://bmdynamics.com/issue_pdf/bmd110587-%2016-39.pdf

Johnson, T. A. 2015. *Cybersecurity. Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*. Published by CRC Press

Karnouskos S. 2011.STUXNET Worm Impact on Industrial Cyber-Physical System Security. *37th Annual Conference of the IEEE Industrial Electronics Society*. http://dx.doi.org/10.1109/IECON.2011.6120048

Kasperski Lab, 2014. Kaspersky Lab Uncovers "The Mask": One of the Most Advanced Global Cyber-espionage Operations to Date Due to the Complexity of the Toolset Used by the Attackers, Available on the Internet: https://kasperskycontenthub.com/wp-content/uploads/sites/43/vlpdfs/unveilingthemask_v1.0.pdf

Kasperski Lab, 2012. Kaspersky Lab Discovers "Gauss" – A New Complex Cyber-Threat Designed to Monitor Online Banking Accounts, Available on the Internet: http://newsroom.kaspersky.eu/fileadmin/user_upload/en/Images/Lifestyle/Kaspersky_Lab_Press_Release_Gauss_-09.08.2012.pdf

Kiškis M.; Limba T. 2016. Biotechnology Patenting in Small Countries—Strategies for the International Marketplace. *Biotechnology Law Report* 35(6): 291-299. http://doi.org/10.1089/blr.2016.29035.mk

Kiškis M.; Limba T.; Gulevičiūtė G. 2016. Business Value of Intellectual Property in Biotech SMEs: Case Studies of Lithuanian and Arizona's (US) Firms. *Entrepreneurship and Sustainability Issues* 4(2): 221-234. http://dx.doi.org/10.9770/jesi.2016.4.2(11)

Kroger W. 2008. Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools, *Reliability Engineering & System Safety* 93(12): 1781–1787. http://dx.doi.org/10.1016/j.ress.2008.03.005

Langner R. 2013. To Kill a Centrifuge, A Technical Analysis of What Stuxnet's Creators Tried to Achieve, Available on the Internet: https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

Law on Cyber Security of the Republic of Lithuania. Available on the Internet: https://www.e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4

Limba T.; Agafonov K.; Damkus M. 2016. Cyber Security: From Technology to Management, *Social Innovations: Theoretical and Practical Insights*, 16th International Interdisciplinary Conference on Social Innovations, September 2016, Vilnius, Lithuania.

Limba T.; Gulevičiūtė G.; Kiškis M.; Romeika G. 2016. E-Business Qualitative Criteria Application: Analysis of Global Market. *Transformations in Business & Economics*: 645-659.

Lithuania National Security Strategy. Available on the Internet: https://www.e-tar.lt/portal/lt/legalAct/TAR.FD615B2F7F90

Lukszo Z.; Deconinck G.; Weijnen M. P. C. 2010. *Securing Electricity Supply in the Cyber Age*. Published by Springer

Macaulay T. 2008. *Critical Infrastructure: Understanding Its Component Parts, Vulnerabilities, Operating Risks, and Interdependencies*. Published by CRC Press

Masero M. 2010. Governance: How to Deal with ICT Security in the Power Infrastructure. http://dx.doi.org/10.1007/978-90-481-3594-3_6

North Atlantic Treaty Organization (NATO), 2010. Active engagement, Modern Defence, Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization, adopted by Heads of State and Government at the NATO Summit in Lisbon. Available on the Internet: http://www.nato.int/cps/po/natohq/official_texts_68580.htm

Organization for Security and Cooperation in Europe, 2013. Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace. Available on the Internet: http://www.osce.org/secretariat/103500?download=true

P.W. Singer P. W.; Friedman A. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Published by Oxford University Press

Radziwill Y. 2015. *Cyber-Attacks and the Exploitable Imperfections of International Law*. Published by Brill/Nijhoff

Rosner K, 2013. Is Information Sharing a Help or Hindrance to Critical Energy Infrastructure Protection? *Energy Security Forum.* Available on the Internet: https://enseccoe.org/data/public/uploads/2017/02/ensecforum8-reduced.pdf

securelist.com, 2013. "Red October" Diplomatic Cyber Attacks Investigation, Available on the Internet: https://securelist.com/analysis/publications/36740/red-october-diplomatic-cyber-attacks-investigation

sputniknews.com, 2008. Russian nuclear power websites attacked amid accident rumors, Available on the Internet: https://sputniknews.com/russia/20080523108202288

Stouffer K.; Falco J.; Kent K. 2013. Guide to Industrial Control Systems (ICS) Security. Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC). http://dx.doi.org/10.6028/NIST.SP.800-82r1

Štitilis, D.; Pakutinskas, P.; Kinis, U.; Malinauskaitė, I. 2016. Concepts and principles of cyber security strategies, *Journal of Security and Sustainability Issues* 6(2): 197–210. http://dx.doi.org/10.9770/jssi.2016.6.2(1)

Techrepublic, 2004. *Disaster Planning and Recovery Pack*. Published by TechRepublic

Ten C.W.; Manimaran G.; Liu C. C. 2010. Cybersecurity for Critical Infrastructures: Attack and Defense Modeling. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans* 40(4): 853-865. http://dx.doi.org/10.1109/TSMCA.2010.2048028

Tvaronavičienė, M. 2012. Contemporary perceptions of energy security: policy implications, *Journal of Security and Sustainability Issues* 1(4): 235–247. http://dx.doi.org/10.9770/jssi.2012.1.4(1)

Tranchita C., Hadjsaid N., Viziteu M., Rozel B., Caire R. 2010. ICT and Powers Systems: An Integrated Approach. *Securing Electricity Supply in the Cyber Age*, Springer: 71-109. http://dx.doi.org/10.1007/978-90-481-3594-3_5

U.S. Department of energy; U.S. Department of Homeland Security, 2006. Roadmap to Secure Control Systems in the energy Sector. Available on the Internet: https://energy.gov/sites/prod/files/oeprod/DocumentsandMedia/roadmap.pdf

Umbach F. 2013. Cyber attacks on critical energy infrastructures are increasing globally, Available on the Internet: https://www.gisreportsonline.com/cyber-attacks-on-critical-energy-infrastructures-are-increasing-globally,defense,818,report.html

United States Government Accountability Office (GAO), 2007. Critical Infrastructure Protection - Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain. Available on the Internet: http://www.gao.gov/assets/270/268137.pdf

US Government Accountability Office (US GAO), 2005. Critical Infrastructure Protection. Available on the Internet: http://www.gao.gov/new.items/d05434.pdf

Vlasenko A.; Limba T.; Kiškis M.; Gulevičiūtė G. 2016. Research on Human Emotion while Playing a Computer Game using Pupil Recognition Technology. *Journal of the Association for Information Communication Technology Education and Science*: 417-423. http://dx.doi.org/10.18421/TEM54-02

Volz D. 2016. U.S. government concludes cyber attack caused Ukraine power outage. Available on the Internet: http://www.reuters.com/article/us-ukraine-cybersecurity-idUSKCN0VY30K

Wang W.; Lu Z. 2013. Cyber Security in the Smart Grid: Survey and Challenges, *Computer Networks* 57(5): 1344–1371. http://dx.doi.org/10.1016/j.comnet.2012.12.017

Water Information Sharing and Analysis Center (WISAC). 2015. 10 Basic Cybersecurity Measures Best Practices to Reduce Exploitable Weaknesses and Attacks. Available on the Internet: https://ics-cert.us-cert.gov/sites/default/files/documents/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_S508C.pdf

Wei D.; Lu Y.; Jafari M.; Skare P.; Rohde K. 2010. An integrated security system of protecting Smart Grid against cyber attacks. http://dx.doi.org/10.1109/ISGT.2010.5434767

The International Journal
ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2017 Volume 4 Number 4 (June)
http://doi.org/10.9770/jesi.2017.4.4(12)

Tadas LIMBA is associate professor at the Mykolas Romeris University (e-mail: tlimba@mruni.eu). He obtained PhD degree in management from Mykolas Romeris University in 2009. He is the head of Joint Study Programs "Informatics and Digital Contents" with Dongseo University in South Korea taught en English at Mykolas Romeris University. His research interests include over than 15 Years of experience in a field of E-Government, E-Business, IT application for the organizational change and Digital Contents. He is actively developing and expanding the relations for the future prospectives of the common activities with Dongseo University. Tadas Limba has over 30 scientific publications on different topics related with New Public Management, E-Government, E-Signature, E-Time Stamping, E-Business, E-Marketing, IT and Patent Law, Biotechnology Strategies. He is also the international expert in a field of E-Government and has trained the Faculty Members of Public Administration Academy of Republic of Armenia and Eurasian International University in Armenia in 2014. Tadas Limba visited Communication University of China in 2014 and had the research internships at Arizona State University, USA and at Dongseo University, South Korea in 2015.
ORCID ID: orcid.org/0000-0003-2330-8684

Tomas PLĖTA is a CIS officer at the NATO Energy security Center of Excellence (e-mail: tomas.pleta@enseccoe.org). His main research interests related to Cybersecurity management of states critical energy infrastructure, also data protection on critical energy IT systems, intellectual property, cyber security, online security issues.
ORCID ID: orcid.org/0000-0002-5376-6873

Konstantin AGAFONOV is a PhD student at the Mykolas Romeris University (e-mail: ka1979@gmail.com). His PhD topic is related to cyber security management for electronical voting systems. His research interests also include information and data security, data protection and cyber security issues.
ORCID ID: orcid.org/0000-0002-8962-0083

Martynas DAMKUS is a lecturer at Mykolas Romeris University (e-mail: martynas.damkus@gmail.com). He is the member of Lithuania Electronic information security (cyber security) Advisory Board. His research interests are related to cyber security and data protection on critical state IT systems, intellectual property, cyber security, online security issues.
ORCID ID: orcid.org/0000-0002-3771-6323