Cyber security management model: A proposal for organizations

Assoc. prof. Ing. Josef Kubík, CSc
Faculty of Administration and Economic Studies in Uherské Hradiště, Města Mayen 1536, Uherské Hradiště 686 01, Czech Republic, e-mail: studium@fves.eu

Assoc. prof. RNDr. Aleš Ruda, Ph.D., MBA
Faculty of Administration and Economic Studies in Uherské Hradiště, Města Mayen 1536, Uherské Hradiště 686 01, Czech Republic, e-mail: studium@fves.eu

Abstract

In this paper, it is confronted a question of cyber security management in organizations. The whole cyber world of today is permanently exposed to various cybernetic threats and attacks, that are more or less sophisticated, structured and have various motivations. No individual nor organization or cybernetic system is perfectly protected. Regarding this, it is essential for organizations to develop an effective and functional cyber security management system to eliminate threats and minimize extent and impact of attacks. The paper proposes a possible way how to manage cyber security in organization. Authors believe that proposed model is applicable for a wide range of organization across economy.

Keywords: cyber security; management; cybernetic threats; ICT
JEL classification: L2

1. Introduction

Why it is important to manage cyber security in organization? Current world is among other characterized by massive development of ICT tools. These tools affect all aspects of human live – professional or personal. In case of organizations embedded in economy, more and more activities and services are realized in virtual environment. Electronation of agendas and tasks is crucial for future organizational development and survival. Respecting all the positives and opportunities of using ICT, significant threats must be considered. Facing threats and challenges in virtual world, effective managerial model for cyber security plays an essential role.

Authors react to mentioned ideas and propose a managerial model for cyber security system that could be applied in organizations across economy. Their aim is not to provide “one size fits all” solution, but to offer lean and functional cyber security management model. This approach seems to be suitable for customization in various organizations. The paper summarizes authors´ proposal and is structured as follows:
The second chapter summarizes theoretical fundamentals of cyber security issues, cyber world in general and issues related to cyber security management.

The third section provides basic internal logics of authors’ work, fundamental questions are formulated respectively.

The fourth chapter introduces the cyber security management model proposal itself. The model is visualized via several objects to be easily interpreted.

The final chapter briefly summarizes and provide some conclusions.

2. Theoretical Basis

Extend and significance (economic or societal) of cyber world (according to Studýnka, 2019 cyber world is an environment of information’s life cycle, parallel to physical world, including information systems, services and infrastructure) and everyday cyber life seem to increase unprecedently in last decades (Uma & Padmavathi, 2013; Pleta et al., 2020) and it is relevant to speak about information society (Studýnka, 2019). Pleta et al. (2020) conclude positives of this fact but also point at risk or threats. Cyber security of virtual systems is a highly discussed and important issue, noteworthy for individuals, organizations, governments and public bodies, economic systems or societies (Fisher, 2016; Mulligan & Schneider, 2011).

To define the term cyber security is many but not easy task. According to Fisher (2016), cyber security consists of protection of computer systems and network resources from attack, damage or interference. Mulligan & Schneider (2011) define cyber security as "the protection of information systems, such as those that support military, financial, or critical infrastructure, from unauthorized access, use, disclosure, disruption, modification or destruction." Fisher (2016) further explains that cyber security is a multidisciplinary field that involves techniques and tools from various domains such as networking, cryptography, and software engineering.

Very important issue, thinking about cyber security, is management of cyber risks and threats. Disturbance of cyber security very often affects safety, accountability, reliability, economy or individual lives and society (Fisher, 2016; Mulligan & Schneider, 2011). And this is the reason why to efficiently manage cyber security systems in organizations. Effective cyber security management system ensures flexible and fast reactions to cyber disturbances, minimizes their impacts and mitigates risks. Effective system management ensures system resilience and fast reactions to cyber threats. Effective cyber security management system ensures system resilience and fast reactions to cyber threats.

To define the term cyber security is many but not easy task. According to Fisher (2016), cyber security consists of protection of computer systems and network resources from attack, damage or interference. Mulligan & Schneider (2011) define cyber security as "the protection of information systems, such as those that support military, financial, or critical infrastructure, from unauthorized access, use, disclosure, disruption, modification or destruction." Fisher (2016) further explains that cyber security is a multidisciplinary field that involves techniques and tools from various domains such as networking, cryptography, and software engineering.

Very important issue, thinking about cyber security, is management of cyber risks and threats. Disturbance of cyber security very often affects safety, accountability, reliability, economy or individual lives and society (Fisher, 2016; Mulligan & Schneider, 2011). And this is the reason why to efficiently manage cyber security systems in organizations. Effective cyber security management system ensures flexible and fast reactions to cyber disturbances, minimizes their impacts and mitigates risks. Effective system management ensures system resilience and fast reactions to cyber threats. Effective cyber security management system ensures system resilience and fast reactions to cyber threats.

To define the term cyber security is many but not easy task. According to Fisher (2016), cyber security consists of protection of computer systems and network resources from attack, damage or interference. Mulligan & Schneider (2011) define cyber security as "the protection of information systems, such as those that support military, financial, or critical infrastructure, from unauthorized access, use, disclosure, disruption, modification or destruction." Fisher (2016) further explains that cyber security is a multidisciplinary field that involves techniques and tools from various domains such as networking, cryptography, and software engineering.

Very important issue, thinking about cyber security, is management of cyber risks and threats. Disturbance of cyber security very often affects safety, accountability, reliability, economy or individual lives and society (Fisher, 2016; Mulligan & Schneider, 2011). And this is the reason why to efficiently manage cyber security systems in organizations. Effective cyber security management system ensures flexible and fast reactions to cyber disturbances, minimizes their impacts and mitigates risks. Effective system management ensures system resilience and fast reactions to cyber threats. Effective cyber security management system ensures system resilience and fast reactions to cyber threats.
undesirable, action (e. g. Mulligan & Schneider, 2011). The aim of cyber security is attacks elimination, via application of effective and functional tools. Cyber attacks can be classified respecting various viewpoints, e. g. purpose (explorative, attacks on access, service denial attacks), legal classification (crime, espionage, terrorism, cyber war), level of agent engagement (active, passive), extend of impacts (extensive severe attacks, attacks with limited impacts), type of network (MANET, WSN) – see Uma & Padmavathi (2013) for more comprehensive overview.

Regarding all the abovementioned ideas, it is possible to summarize several challenges of cyber security and its management (based on Fisher, 2016; Mulligan & Schneider, 2011 or Wirtz & Weyerer, 2007):

- Accurate and effective structure and security safeguards implemented in ICT systems.
- Adequate and periodic investments into cyber security systems and tools.
- Agreement upon valid and integrated definition and perception of cyber security.
- Minimization of lag between cyber criminality and security reactions; effective prevention.
- Managerial, political, legal, economic, and public support and understanding the significance of cyber security; overall enlightenment, awareness, and education.
- Change resistance overcoming.

2.1 Management of Cyber Security

Business and managerial models are changing regarding increasing number of virtual activities and operations (Andronache & Althonayan, 2019). This brings significant benefits, but on the other hand also lots of threats - Andronache & Althonayan (2019) mention term “development paradox”; and intensification of cyber attacks that are sophisticated. Regarding this, cyber security management is required to ensure adequate system protection, resiliency, integrated strategies and suitable operative models, proactive safeguards, as well as periodical evaluation and prospective change (Ezingeard et al., 2007; Limba et al., 2017). On the other hand, organizations and management are not effective in these issues (see, e. g. Andronache & Althonayan, 2019; Ezingeard et al., 2007; Tisdale, 2015 for this thesis), however management is usually aware of their importance; sometimes this lead also to undesirable overreaction and over-engineering of solutions (Ezingeard et al., 2007).

According to Tisdale (2015), arguments for complex and effective cyber security management are obvious – overcoming fragmentation of cyber security systems, reduction of costs of cyber incidents, operational trade-offs, vulnerabilities adaptation and resistance, keeping up with changes in environment, technological development, organizational success and survival.
Cyber security management can be perceived as:

- Holistic, strategic system, overcoming so called “silo” approaches to cyber security in organization, for effective organization-wide risk governance, that is subject of internal and external pressures and changes (Andronache & Althonayan, 2019; Ezingeard et al., 2007). Limba et al. (2017) mention that cyber security management consists of regulation, governance, risk management, security culture, technology management, incident management.

- Comprehensive processional approach including security policies, education, training, awareness, security monitoring focusing on safeguards of information systems and cyber assets important to success and survival of organization, reducing non-compliance behaviour (Chen et al., 2015).

- Managerial system including reporting, policy setting, organizing, analysing, mitigation of risks, resiliency, interconnectivity and partnership, controlling, accountancy, decision-making, risk management, evaluation, and modification (Andronache & Althonayan, 2019; Ezingeard et al., 2007).

- Multi-dimensional and multi-genre mechanism fulfilling technical, societal, operational, economic, value-protective functions as well as enhancing added-value of activities (Andronache & Althonayan, 2019; Tisdale, 2015).

- Part of overall organizational strategy, related to objectives achievement and solving social as well as organizational and economic nature of cyber security problems (Ezingeard et al., 2007).

- System, how to build effective cyber security processes for systems and information protection (Ezingeard et al., 2007).

In table 1 it is summarized several cyber security management system components.

**Table 1: Components of cyber security management system**

<table>
<thead>
<tr>
<th>Determinants of cyber security management</th>
<th>Benefits of cyber security management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizational determinants:</td>
<td>Better and more conscious compliance of cyber security rules</td>
</tr>
<tr>
<td>- Initiative and support of management and other internal stakeholders, combination of top-down and bottom-up approaches</td>
<td>Competitive advantage from economic and values’ meeting viewpoint</td>
</tr>
<tr>
<td>- Positive organizational culture and trust, communication, transparency</td>
<td>Resilience and better change or crisis adaptation</td>
</tr>
<tr>
<td>- Clear competencies and responsibilities</td>
<td>Organizational and process effectiveness and coordination</td>
</tr>
<tr>
<td>- Awareness of cyber threats</td>
<td></td>
</tr>
</tbody>
</table>
- Integrity of organizational and security objectives
- Existence of conceptual documents, methods, and legislation
- Formalization of processes and standards

Leadership enhancement and proactive approach to strategic and operational issues
Reduction of values and goals discrepancies

External determinants:
- Number and complexity of cyber threats
- Regulations and requirements of external stakeholders
- Accepted standardization and its positive reputation

Reduction of informational rush, misunderstandings, and biases
Higher internal and external stakeholders’ satisfaction and motivation

<table>
<thead>
<tr>
<th>Barriers of cyber security management</th>
<th>Maturity of cyber security management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Related to human resources:</td>
<td>Cyber security is not managed in holistic way and is lagging threats and current level of cyber crime</td>
</tr>
<tr>
<td>- Internal culture that is not cyber security supportive</td>
<td>Organization do not have sufficient control and risk management mechanisms</td>
</tr>
<tr>
<td>- Lack of awareness and competencies for work in cyber environment</td>
<td>Management of organizations understand and support generally the idea about quality of security management and cyber security systems</td>
</tr>
<tr>
<td>- Change resistance</td>
<td>Lack of resources and skills</td>
</tr>
<tr>
<td>Related to strategy:</td>
<td>Organizations are aware of priorities formulation, strategies formulation, evaluation of performance, education, and enlightenment</td>
</tr>
<tr>
<td>- Costs of cyber security systems</td>
<td></td>
</tr>
<tr>
<td>- Underinvestment into cyber security infrastructure due to underestimation of its significance and returns</td>
<td></td>
</tr>
<tr>
<td>- “Silo” structures instead of complex structures</td>
<td></td>
</tr>
<tr>
<td>- Lack of maturity and preparedness, reactivity</td>
<td></td>
</tr>
<tr>
<td>- Low prediction ability and understanding to global complex environment</td>
<td></td>
</tr>
</tbody>
</table>

Source: based on Andronache & Althonayan (2019); Ezingeard et al. (2007); Chen et al. (2015); Tisdale (2015); Niekerk van & Solms von (2010).

Building effective cyber security management model, it is important to overcome several common mistakes (see, e.g. Limba et al., 2017) – firstly believe that systems can be resistant to any vulnerability and be fully safe; secondly believe that hiring best experts can provide absolute safety of systems; thirdly believe that using the latest and most expensive or appreciated security technologies can provide 100% security; fourthly believe that cyber security is prominently about monitoring and control; fifthly believe that used security measures are the best.

3. Methodology: Approach to model development

How to develop a cyber security management model? Seemingly a simple question, but in fact it is far from reality. To handle this essential question, the methodology of authors’
approach is now to be introduced. At the beginning of whole process authors tried to react to following issues:

What are the main needs of organizational cyber security; what are the main weak and strong points? To answer this, the initial analysis of systems needs to be applied.

Who is going to manage cyber security in organization? The competencies and responsibilities need to be clarified.

Does organization have sufficient hardware, software and economic sources? Potential investments need to be considered.

How does organization manage its cyber security? Strategies, policies, and methods need to be formalized and standardized. This is an issue of prevention.

How does organization manage the impacts of cyber attack? The process needs to be formalized and standardized. This is an issue of minimizing negative impacts of successful cyber attack.

Abovementioned issues were critically assessed by the authors, regarding either current surveys (their main findings and opinions were introduced above in the second chapter of the paper), or practical experience of authors and several other experts interviewed. Such approach was found appropriate, especially due to variation in opinions and attitudes of sources.

Based on introduced approach, authors target main purpose of this paper – how to effectively and fluently develop and apply a model for cyber security management. Proposed model is realized internally with minimum additional sources requirements. Even though, it is perfectly competitive, lean and functional, closely connected with overall structure of organization and its management system. Authors add also several considerable remarks for organizations that outsource their ICT systems.

Authors believe in practical applicability and appropriateness of proposed model for cyber security management but are aware of its limitations and individual adjustment requirements.

4. Cyber security management model proposal

In this chapter, authors introduce the actual model proposal for cyber security management – thus, here is embedded the core of this paper and the whole work. Firstly, the model is visualized in figure 1.

In the first phase, a comprehensive analysis of current situation of cyber security and its system should be developed. Based on organizational data and experience, the organization gains wide range of information and will be ready to develop effective managerial system for cyber security. A key point is to base the analysis on evidence-based approach – IT department of the organization should mine all available data about cyber security and ICT systems (among others revise access rights and rules, safety nets,
Software equipment, etc.) Suitable can be formulation of SWOT analysis that concludes all the relevant information and is user friendly for experts as well as for laiks. Results should be disseminated through whole organization if it is relevant from managerial viewpoint.

In the second phase, management should nominate members for cyber security executive board (CSEB). This body will be responsible for effective and actual cyber security system which is flexible and able to react to the needs of organization and internal or external changes. It would be convenient to develop a periodic schedule of CSEB meetings. The possible structure of the body is illustrated in figure 2. Key operational and expert role should be dedicated to the manager of cyber security and to IT department. Managers and employees from other departments should provide necessary and desirable cooperation and keep themselves informed about actualities. Additionally, independent cyber auditor and manager of data protection regulation (where applicable) should be nominated, outsourcing is a relevant option.

In the third phase, required sources (economic, personal, technological and others) need to be identified and ensured. Screening of needs and actual situation is a task especially for IT employees; following assurance of necessary resources is a task for management, CSEB respectively.

In the fourth phase, it is useful to support the whole cyber safety system by its formalization and standardization. This could be done via formulation of cyber security strategy and policy, as well as via formulation of process maps and understandable internal legislation. Preparation and final results of these activities should be discussed with employees and these should be kept informed about all relevant facts. Thus, acceptation and adoption of good praxis will be higher, and engagement of all employees will be better. In this phase of the process, all employees should already know their competencies and responsibilities, which should be implemented into their everyday work. This phase is the main part of strategic and operational management of cyber security in organization. Let us stress once again at this point, communication and acceptation are crucial for all cyber security activities and activities in ICT systems in general. Important part of standardization and formalization of cyber security system should be planning and realization of suitable education, enlightenment, and awareness of individuals enhancement. Managerial support is the other cornerstone.

In the fifth phase, the system of reaction to cyber attack (or incident, more generally) should be developed and formalized. Authors of this paper recommend formulate a process map with essential steps, that could be more precisely described in internal legislation, cyber security strategy and policy (see phase four). Simple structure of such process map is introduced in figure 3.

One key characteristics of a model proposal lefts – periodicity and modifications. Like many other models or systems, even the system of cyber security management should be viable, flexible, and evolving. Regarding this, it should be standardized a periodicity of phase one of the model (analysis) to ensure validity and topicality. According to periodically identified and evaluated findings, modifications of phase three and four should be realized. In case of phase five, this one is operative and crisis solving. Regarding this, it should be flexible, accurate, as well as swift; the organization and all individuals should learn from various crisis situations and try to be better in future.

DOI: 10.60026/IJPAMEDv8i2.140
Figure 1: Cyber security management system development

<table>
<thead>
<tr>
<th>1. What</th>
<th>Comprehensive analysis of current state of art</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Who</strong></td>
<td>Management of organization</td>
</tr>
<tr>
<td></td>
<td>IT employees or external experts</td>
</tr>
<tr>
<td><strong>How</strong></td>
<td>Audit of cyber systems, processes and roles – data and process analysis</td>
</tr>
<tr>
<td><strong>Result</strong></td>
<td>Report with clear and sufficient information about strong, weak points, threats and opportunities</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2. What</th>
<th>Cyber security executive board (CSEB) Competency and responsibilities model</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Who</strong></td>
<td>Management of organization</td>
</tr>
<tr>
<td></td>
<td>Personal department</td>
</tr>
<tr>
<td><strong>How</strong></td>
<td>Formation of CSEB and nomination of members</td>
</tr>
<tr>
<td></td>
<td>Analysis of positions characteristics in organization</td>
</tr>
<tr>
<td><strong>Result</strong></td>
<td>Functioning CSEB</td>
</tr>
<tr>
<td></td>
<td>Positions´ characteristics adjustment</td>
</tr>
<tr>
<td></td>
<td>Competencies and responsibilities are clear, people know what to do in daily work</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3. What</th>
<th>Ensured resources</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Who</strong></td>
<td>CSEB</td>
</tr>
<tr>
<td></td>
<td>IT employees</td>
</tr>
<tr>
<td><strong>How</strong></td>
<td>Analysis of needs and current sources revision – data analysis</td>
</tr>
<tr>
<td><strong>Result</strong></td>
<td>Resources are available, sufficient and actual</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4. What</th>
<th>Strategies, politics and methods</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Who</strong></td>
<td>CSEB</td>
</tr>
<tr>
<td><strong>How</strong></td>
<td>Formulation of concept documents and methodologies</td>
</tr>
</tbody>
</table>
Formulation and standardization of objectives and activities

| **Result** | Formal system and processes are developed and agreed across organization  
People know what to do in various situations in cyber space  
Process maps and internal legislation is developed |

| **5: What** | **Cyber attacks situations** |

| **Who** | CSEB  
IT employees |

| **How** | Formulation of process maps and internal legislation  
Cyber security technologies application |

| **Result** | Process of cyber attack solution is formalized  
People know what to do in case of cyber attack |

Source: Authors.

As mentioned above, key professional role in CSEB should be dedicated to manager of cyber security. Regarding the expert aspect, head of IT department could be suitable candidate. His duties should be related to coordination of cyber security activities, resources allocation, analyses and formulation of requirements or recommendations, strategic planning of cyber security, operative and risk management in cyber security affairs.

On the other hand, chair of CSEB should coordinate activities of CSEB with all other activities within organization, link management structure with CSEB, provide resources, make most important strategic decisions and solve prospective conflicts. Executive manager of organization could be one of suitable candidates for this position.

Role of particular managers of other departments is more or less supportive. These managers should provide required information and cooperate with manager of cyber security, IT department consequently; prospectively they participate at strategic planning, risk management and decision-making processes.

Relatively specific and more ad hoc character have cyber auditor and manager of data protection regulation. Cyber auditor should be, without any doubt, independent person – if not, proper picture of cyber security situation in organization could not be provided. Independence of cyber auditor can be ensured via creation of a specific job position.
outside the system of organizational departments, sufficient financial reward at the position; could be strengthened via outsourcing of the auditing service.

Manager of data protection regulation can be constituted or not (in lots of organizations, there is no such need identified). Management of data protection is, on the other hand, very important issue, when organizations administrate wide range of sensitive data, as well its important role play also legislative requirements. Thus, it could be advised to keep establishment of this function in mind, it is also possible to outsource the service.

**Figure 2: Possible structure of CSEB**

![Possible structure of CSEB](image)

Source: Authors.

Every step of the process of cyber attack (incident) management has its importance and it is not advised to miss or omit some of them. Immediate notification about attack or even suspicion is crucial for effective solution of crisis and elimination of negative impacts. Every person in organization should be aware of this fact and know to whom give information. IT specialists and manager of cyber security are mainly responsible for situation analysis, operative actions and arrangements or prospective reduction of cyber services and activities realization. After primer appropriate arrangements and actions, the CSEB should discuss the situation, consider objectives, future steps and recommendations proposed by manager of cyber security. Accordingly, decisions should be made, and recovery plan should be agreed. Very important part of the process is realization of suitable actions and adjustments of ICT systems; evaluation of crisis; as well as conclusions formulation and learning from failings; prospectively sanction personal failures. In case that cyber attack (incident) is relevant for external subjects (e. g. distortion of clients or supplier’s data; reduction of cyber services provided etc.), it is advised to inform such stakeholders about situation and its solutions.
Finally, authors would like to mention one more issue – outsourcing of the whole ICT system of the organization. Many, especially small or medium-sized organizations do not administrate their ICT systems on their own. They prefer turn-key solutions based on complete outsourcing that is cheaper and more comfortable for them (they do not need IT department, perform savings in personnel, software and hardware equipment etc.). Similar approach prefer e. g. organizations in public sector (see, e. g. Studýnka, 2019 for further discussion) – they need sophisticated systems for administrations of wide range of important data, system compatibility, realization of specific services and activities etc. In house solutions are for them costly and require highly skilled experts.

Regarding above-mentioned issues, organizations should not resign on effective system of cyber security management, but the contrary in fact. If outsourcing ICT systems delivery, organization loses significant part of control and management ability. Authors see threats related to:

- data leakage and fraud
- system gaps which the organization is not familiar with
- overpricing of outsourced services
- unfamiliar safeguards
- delivery of services that do not fit perfectly to needs of organization

Source: Authors.
Proposed cyber security management model is however suitable even for organizations with outsourced ICT systems. Chair of CSEB and manager of cyber security have to be perfectly familiar with supplier conditions and safeguards system; manager of cyber security have to be perfectly familiar with technical solutions of ICT systems; chair of CSEB should strictly require security guaranties in supplier contracts. Open and intensive communication between organization and ICT supplier is crucial.

Authors foresee following modifications of proposed model in case of ICT systems outsourcing:

- Analytical phase is embedded especially into revision of supplier contracts, needs of the organization; additionally, into analysis of ICT systems themselves, if the organization can technically and professionally do so (otherwise, it is possible to ensure professional external audit).
- It can be beneficial to nominate a representative of ICT supplier to CSEB.
- Resource planning should perfectly calculate advantageousness of outsourcing.

Strategies, policies, methods, and internal legislation should be customized to a specific supplier relations and conditions. Every person in organization should nevertheless still clearly know what to do in everyday work, regarding cyber security. All the internal documents should respect organizational needs as well as supplier contracts conditions.

In case of cyberattack (or suspicion), immediate notification and intensive communication with supplier is crucial. This communication is under manager of cyber security responsibilities. Solution of cyber attack, or incident respectively, is under supplier’s responsibility (regarding contracts), organization should collect all accessible information and evidence related to attack and support the supplier. CSEB should be kept informed, as well as all the persons in the organization, respecting their positions and working tasks. Manager of cyber security in cooperation with supplier should formulate the final report, including causes and impacts of the attack, solutions and future safeguards and objectives. Organization should consider prospective sanctions against supplier or even change of supplier (respecting contracts and circumstances of the cyber attack).

5. Conclusion

The paper introduces several issues related to cyber security and its management in organizations of current world. At the first section of the paper, context of cyber security and cyber attacks (or incidents to be more general) was summarized, followed by ideas regarding management of cyber security. The next section briefly introduced methodology of cyber security model proposal and its internal logics. In the most important section, the model proposal was described and supplemented by several commentaries of authors.

It is noteworthy to mention, that it does not exist one universal solution for development and application of cyber security management models. Every organization should customize the system to its needs and possibilities, as well as to current external
environment. Most importantly – every organization should be aware of its cyber security and apply relevant objectives.

Authors’ aim was not to force organizations into any universal model fit, but to provide some useful ideas for management of cyber security, that they consider to be crucial in current world. Proposed model pointed at several systematic issues not to be overlooked. Nevertheless, there could be limitations identified, related e.g. to model’s applicability in various organizational environments, specified details of partial phases, roles of CSEB members and their number etc. This is an issue for future work. On the other hand, simplicity and general guideline character of proposed model should be evaluated as beneficial, providing wide adjustments possibilities. Such nature of proposed model is its strong and competitive point. Hopefully, in this manner will be the paper and model proposal perceived by readers.
References


