Education in Management of Cybersecurity

Nedko Georgiev Tagarev[1]

University of National and World Economy, Bulgaria[1]

Abstract

The problem presented in this article is the growing need for adequate and relevant cybersecurity education. Current trends placed cybersecurity and the upward trend in the use of smart technologies as the backbone of any business and management education. The education program and training have to cover the specific needs for management of cybersecurity. The program includes – computer security, network security, information technologies (IT) security, physical security, Internet security, security policy, management and business continuity. For training and analyses, we use cyber-attacks examples and real-life cases. As a milestone, the author, use the cybersecurity in objects of critical infrastructure. These objects require specific cybersecurity measures and defence mechanisms. This education of management of cybersecurity provides the often forgotten "horizontal approach" in cybersecurity. On the other side, in general, there is a need for adequate analyses – methods and methodology. The most frequently used, training methods are risk analyses, case studies and scenario analyses. Information security (IS) is part of cybersecurity education. Education in IS is based on most popular international standards such as ISO and NIST. Education relies on Information security management system (ISMS), cryptography, authentication methods and process analyses.

Keywords: *Cybersecurity, Management, Education*

1. Introduction

The main *problem* in education process or program is the complexity of the management of cybersecurity. This problem is a result of two main issues – the minimum requirements for some information technologies knowledge and the interconnection between all the studied topics in cybersecurity management. We can see the main topics in Figure 1. The education of cybersecurity has to be *adequate* to the current situation and usage of information technologies in the word. In the near past usage of digital data was rare and specific for some activities. Now it is rare to see human activities without computers as the trend shows a move from the desktop to mobile devices. We take this in mind when it comes to education in cybersecurity. For example, there is such a rise for science -8% and education – 5%[1]. In addition, the education of cybersecurity has to be *relevant* to the cybersecurity laws, regulation, standards and national policies. These laws and regulations are the results of a rising number of attacks and cybersecurity incidents. For example, in 2017, the IoT attacks raised up with over 600% and the ransomware attack raised more than 350 times[2]. The laws and regulation vary from the state(New York's regulations for the financial sector[3]), through international (for example -The General Data Protection Regulation (GDPR)) to national(for example - Cyber Security Act in Bulgaria[4]). There is another problem concerning the implementation of cybersecurity measures in an organisation. These measures have to be understandable and acceptable. Overall, they should not interfere with business processes.

The *object* of this article is *cybersecurity management* and the *subject* is the *education process*. The *scope* of this paper is limited to the management of cybersecurity and the author did not discuss any technical or technological problems. In addition, the Internet refers to a network.

The *goal* of this article is to present a model for the program for cybersecurity management education. In addition to show some ways to reduce the problems in the complexity of learning. This goal will become more important in a complicated system with the implementation of IoT and smart cities as common practice. Now the biggest challenge for cybersecurity education is the implementation of good practices in the objects of critical infrastructure or in places containing critical information.

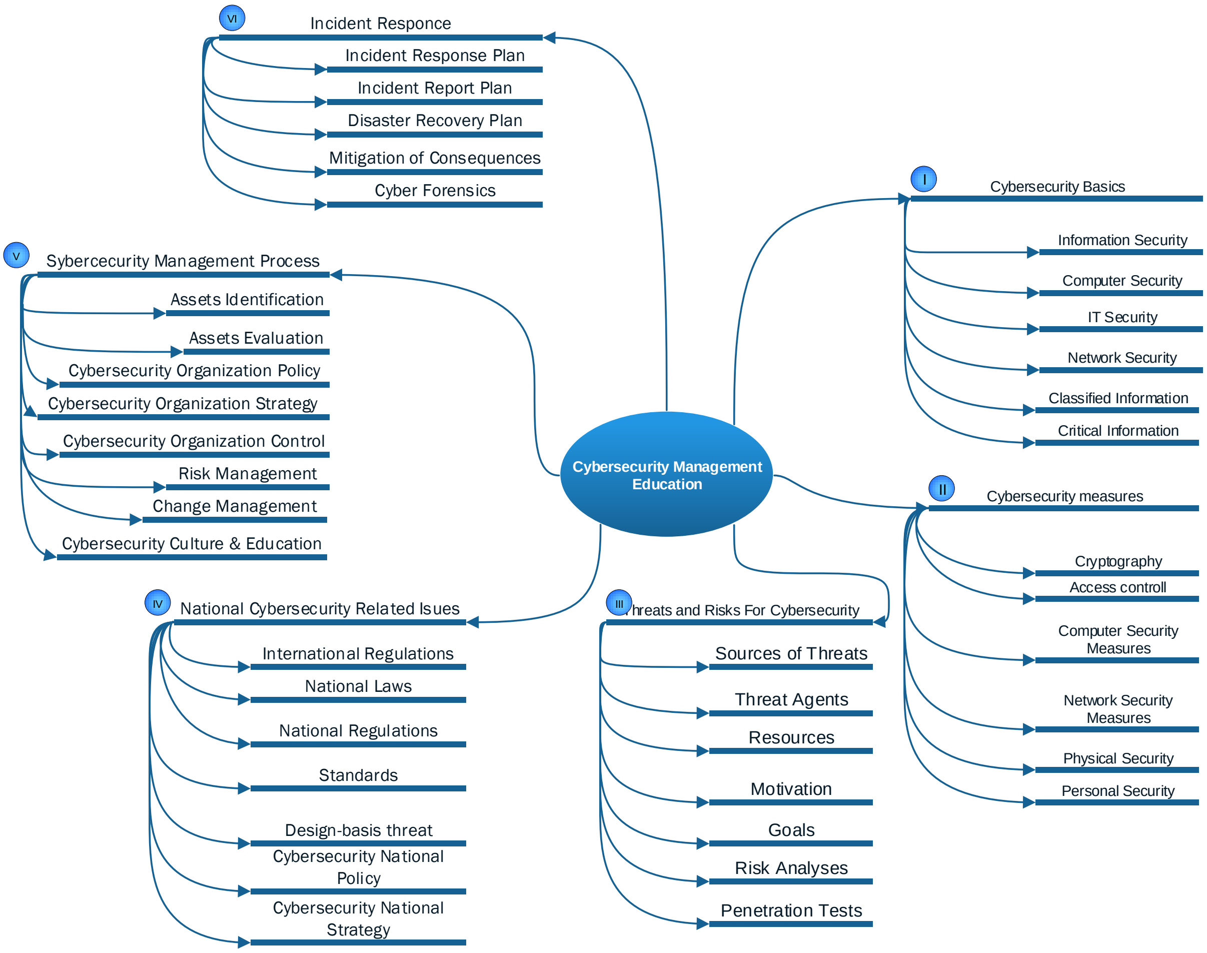

Figure 1. Main topics in cybersecurity management education

2. Cybersecurity basics, cybersecurity measures, cybersecurity threats and risks

The requirements for security or cybersecurity managers are bigger than the requirements for the close specialist, like programmers, system administrators, technicians and engineers. The cybersecurity manager has to have knowledge about – information technologies, cybersecurity, national policy, laws and regulations, economy and management. To obtain this knowledge there have to be clear and systematic education. The first three steps of learning are an interconnected process.

We can present it simple in Figure 2.

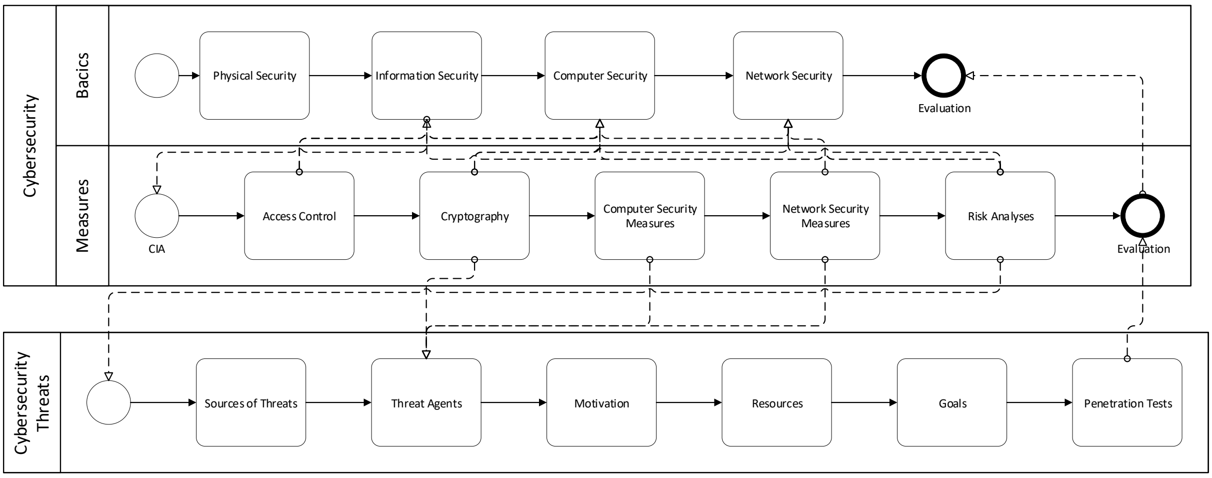

Figure 2. Education in cybersecurity basics process

Physical security is essential to cybersecurity. There are two main aspects that are often forgotten by cybersecurity experts. 1) The physical access to data storages and 2) Lifecycle of data storages. The first aspect is covered in most of the cases by the physical security policy of the organisation. It is based on defence in depth principle. The second aspect of physical protection is often neglected. In many cases, we forget about the lifespan of data holders. For example for HDD most common is 5 years for SSD 7-8. Before the end of this period, they have to be replaced.

Cybersecurity is a more general term that includes *information security(IS)*. IS is the base for cybersecurity education. IS provides the terminology and knowledge of the assets that have to be protected. IS protects the organization's data from unauthorized access or modification to ensure its confidentiality, availability, and integrity(CIA)[5]. There are popular standards that are implemented as management practice and requirements for information security and cybersecurity in general. The most popular are the ISO 27000[6] series and NIST SP 800 series[7]. These standards and principles have to be considered in cybersecurity education.

“*Computer security*, the protection of computer systems and information from harm, theft, and unauthorized use. Computer hardware is typically protected by the same means used to protect other valuable or sensitive equipment...”[8] Computer security is based on three main principles (1) Prevention - Setting up measures to protect against threats. (2) Detection - Have measures and processes in place to detect (on-going) threats. (3) Response - Have processes and instructions in place to react properly on threats. In the education process, these principles have to be explained with security measures.

Network security is the practise of securing a computer network from intruders, whether targeted attackers or opportunistic malware.[9]

We build up *security measures* according to the security threats[10], risk analyses and evaluation of risk. In the curses often, we study the most popular once:

- Probing - Identity listening (or active) communication services.
- Sniffing: Read data from the wire literally without leaving a trace to the sender or receiver.
- Man-in-the-middle - Technique either to read or to manipulate communication between a sender and a receiver literally without indicating an interception to the communication partners.
- Denial-of-service (“flooding”) - Technique to disrupt a communication flow by overloading the communication channel or mechanisms.
- (Computer) Viruses (aka malicious software or malware) - Software program used by attackers to infect a computing device.
- (Computer) Worms - Sub-category of viruses which infects a computer system and then distributes itself to another computer system in order to infect them.
- (Computer) Trojan horses - Sub-category of computer viruses, which indicate the objective of the virus: to pretend to a user of a computer to do something useful or harmless.

Often we forget about social engineering as a main driver for the successful attack. To observe these practices most common we use case study analyses.

We can find most of these threads implemented in national cybersecurity policy or strategy. Also on the national level for objects of critical infrastructure, there are Design Basis Threats[11], which is implemented in the basic education in all of the topics – physical, computer, network etc.

The two most popular security measures that are common for all the systems are – access control and cryptography. The students and security managers have to understand the importance of Identification → Authentication →Authorization and Accountability. Depending on the object, the standards require 2-3 factor authentication. We can choose from something that we know, something that we have and something that we are. This depends on the critical level of information and economic evaluations. For authorization, we have to keep up to the principle of “least privilege”. For managers, teachers demonstrate cryptography through the provided products.

In the aspect of network security measures, the most important thing is the segregation of networks based on their intended purpose. This segregation is a result of assets evaluation. We segregate network with – firewalls, VPN, gateways, demilitarized zones etc. In this point, the students have to gain knowledge of the organization digital infrastructure and they have to differ and recognize its components.

3. Policy, management and incident response

Management of cybersecurity connects to the 1) Management of the process and 2) Organization of personal. There are three approaches to the process:

- Proactive – related to assets evaluation, risk analyses and implementing of security measures.
- Reactive (incident response) – procedures and reports for mitigation of the consequences.
- Crisis management implements the Disaster Recovery Plan and Disaster Recovery System.

Disaster recovery system refers to backup. It depends on the financial capabilities of the organization.[12]

Another important step of management of cybersecurity in an organization is the asset evaluation. If critical assets are not protected this can lead to loss of finances, reputation or problems with the law. The assets differ in structure from site to site. There is a huge difference for example in digital infrastructure that implements an Industrial Control System.

The organization includes the roles and responsibilities of personnel. This also includes personal security (protection of the organization from its employees). Some reports say that 58% of incidents are from insiders for 2018[13].

Cybersecurity policy is the most important document related to – assets, resources, roles and responsibilities of personnel, procedures, change management and incident response. The policy is also obligated to the laws, regulations and standards (Figure 3).

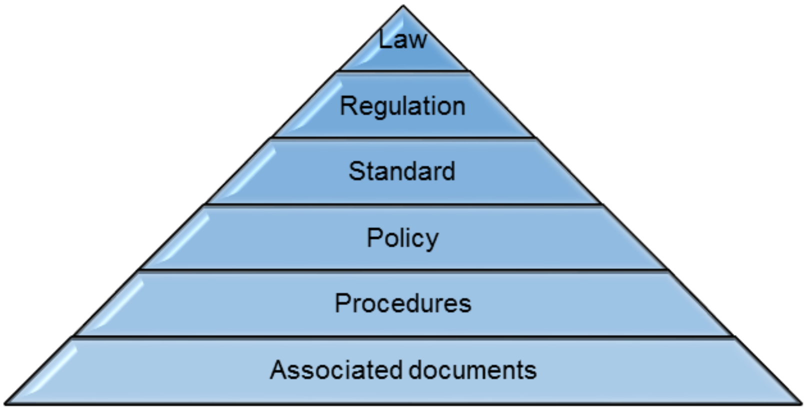

Figure 3. Importance of regulations.

4. Conclusions

Education in cybersecurity is a complex process. It is multidisciplinary, so there has to be a specific approach. We can make several main conclusions:

- Even that the different objects are divided there have to be made a clear connection between topics. For example, cryptography is a security measure for computer security and network security. The same is for access control. Practice shows that confusion arises if we discuss some security measures on one topic.

- It is not of great importance from which module we will start the education process. There is a connection between all of the modules, so there have to be references in each of the topics.
- The education program has to be in accordance with legislation and regulations. The laws and regulations depend on the country so there is no universal approach to this problem.
- Cybersecurity management has to start with assets evaluation. What we are going to protect? The next step is how we are going to protect it?
- Cybersecurity managers have to recognize the different elements in cybersecurity infrastructure.
- In most of the cases, Disaster Recovery has more economic issues than cybersecurity ones.

References

[1] "See Our 2018 Study of Mobile vs Desktop Usage," *Stone Temple*, 01-May-2018. [Online]. Available: https://www.stonetemple.com/see-our-2018-study-of-mobile-vs-desktop-usage/. [Accessed: 04-May-2019].

[2] R. S. Updated: 4/17/2019, "60 Must-Know Cybersecurity Statistics for 2019," *Inside Out Security*, 17-May-2018. [Online]. Available: https://www.varonis.com/blog/cybersecurity-statistics/. [Accessed: 04-May-2019].

[3] "What is the NYDFS Cybersecurity Regulation? A Cybersecurity Compliance Requirement for Financial Institutions," *Digital Guardian*, 04-Feb-2019. [Online]. Available: https://digitalguardian.com/blog/what-nydfs-cybersecurity-regulation-new-cybersecurity-compliance-requirement-financial. [Accessed: 04-May-2019].

[4] "Bulgaria adopts new Cyber Security Act." [Online]. Available: http://www.cms-lawnow.com/ealerts/2018/11/bulgaria-adopts-new-cyber-security-act. [Accessed: 04-May-2019].

[5] "What is information security? definition and meaning," *BusinessDictionary.com*. [Online]. Available: http://www.businessdictionary.com/definition/information-security.html. [Accessed: 17-Nov-2018].

[6] "ISO/IEC 27005:2008," *ISO*. [Online]. Available: http://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/04/21/42107.html. [Accessed: 03-Dec-2018].

[7] T. A. Allen, "NIST Special Publication 800-series General Information," *NIST*, 21-May-2018. [Online]. Available: https://www.nist.gov/itl/nist-special-publication-800-series-general-information. [Accessed: 03-Dec-2018].

[8] "Computer security," *Encyclopedia Britannica*. [Online]. Available: https://www.britannica.com/technology/computer-security. [Accessed: 17-Nov-2018].

[9] "What is Cyber Security? | Definition | Kaspersky Lab." [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security. [Accessed: 17-Nov-2018].

[10] N. Tagarev, "Threats to Information Security," in *East-West Defence and Security Co-operation Part 1*, Sofia, 2015.

[11] "Design Basis Threat (DBT)." [Online]. Available: http://www-ns.iaea.org/security/dbt.asp?s=4. [Accessed: 19-Nov-2018].

[12] N. Tagarev, "System recovery management basics," *4TH Int. Conf. Appl. Inf. Commun. Technol. Stat. Econ. Educ. ICAICTSEE – 2014 Oct. 24-25TH 2014 UNWE SOFIA Bulg.*, no. 4, 2018.

[13] M. Noll, "Insider Threat Statistics: 2018 Research Reports and Surveys," *IT Security Central - Teramind Blog*, 03-Apr-2018.