CYBERSECURITY EDUCATIONAL PROGRAMS: COSTS AND BENEFITS

Dumitru Daniel[1], Ion Tiberiu[2]
[1) 2)] *Carol I National Defence University, Bucharest Romania*
E-mail: dumitru.daniel@unap.ro; E-mail: ion.tiberiu@unap.ro

Abstract

The 21st century is characterized by the emergence of cyberspace as a new frontier, that fundamentally transforms the global economy and the society itself, through the possibility of instant access to information, by facilitating global communications, as well as creating multiple economic opportunities. The globalization of virtual space brought highlighted the lack of international cooperation in the development of unitary cyberdefence strategies.
In this context, both public and private organisations put effort in creating a safer cyberspace, by trying to prevent an action before recovering from an impact. In this sense, the cost of cybersecurity is analysed by reviewing different researches and confronting them with general economic hypothesis, in order to better understand how can a cyberattack be measured.
Even if, no official standard has been yet adopted in order to measure and control the costs associated with implementing cybersecurity programs, in contrast with the potential costs of cyberattacks, multiple studies have analysed different scenarios, resulting in measuring patterns and models. So, what are the main constrains that organisations face when dealing with cybersecurity? How are these constrains interconnected and how can they be measured?
Thus, the present paper aims to highlight some possible responses for these questions in terms of a cost-benefit approach, by highlighting the need of an educational model in order for organisations and countries to have more and better trained specialists.

Keywords
Cybersecurity, data integrity, cybersecurity costs, preventive actions

JEL Classification: F52, M15, O32, O38

Introduction

Cybersecurity can be defined as a set of actions taken by organizations in order to protect from cyberattacks all Internet-connected systems, starting with hardware and software resources, as well as data (information). Taking into consideration the increasing number of cyberthreats, a need for cybersecurity regulations is highlighted by various organizations and governmental bodies in order to create a common language in protecting the cyber environment by using modern information technology.
But, developing the necessary technology that can prevent or efficiently react to cyberattacks in order to protect the integrity, availability, reliability and confidentiality of information involves multiple resources that can be measured in time, human resources and money. When talking about cybersecurity costs, most studies focus on costs from a financial

perspective, more exactly: budgeting a prevention strategy and determining the economic impact of a cyberattack (Benton and Radziwill, 2017).
Different perspectives in measuring the costs of cybersecurity have been presented in multiple studies, starting with the introduction of the concept of "cyberquality" in 1995, by The American Society of Quality. Other theories build different models on cost estimation by using resources from other domains, for example Campbell (2003) and Gordon (2011) examined the financial impact of cyberthreats by using a stock market performance model.
In this context, the present paper represents an exploratory attempt to identify different perspectives regarding cybersecurity in terms of costs and benefits. Thus, the research methodology is based on a literature review in order to highlight the importance and role that resources invested in the cybersecurity sector have, from a preventive point of view, the main goal being to make it easier for organizations to study, monitor, and control the costs associated with cybersecurity.

1. Analysis of cybersecurity good practices across different industry sectors, government and military structures - A literature review

The Information Technology and Communications (IT&C) sector has registered a fast and complex evolution in the last decades, information exchange and communications becoming a very important resource for society and the individual itself. Information stored and processed on computers became so important for the modern society that its confidentiality, integrity and accessibility must be trustworthy in order for international, regional or national fundamental structures to function.
For example, if a bank's database, which holds all the sensitive information regarding its customers, is corrupted, the bank's will be ruined as a business and, in a best-case scenario, refunds will be provided for this error. Thus, the solution will involve huge financial costs, for all involved parties, the bank, the clients, insurance companies etc. But, when talking about classified information, stored on military servers, its loss will have a strong impact on national or international security, for a certain country or a region, involving multiple costs for all impacted bodies, not just financial ones.
Perspectives regarding the financial costs of cyberattacks, the increasing cyber threats associated with the growth of cyber-crime organizations, all these aspects illustrate the need for an intelligence-led solution that can address these rising challenges. In the need for a more complex methodology to fully comprehend cyber threats, the real costs associated to them and the potential damages that these attacks can generate, multiple researches have been made, from the academic environment, to military research, multiple IT global businesses being involved, as in the end everyone can be a potential target.
One of the reports that highlight society's critical needs is published by Intelligence and National Security Alliance (INSA) Cyber Council (2011). This subject is analyses having as a central hypothesis that critical infrastructures are at significant risk to this modern form of warfare. Much of the world's critical infrastructure, including the energy sector, finance or transportation sector, was created and netted before these security risks became apparent. Even if all critical infrastructures have implemented security features, many still remain vulnerable to attackers, as legacy software (which is still popular in many organizations) can provide trap doors to an apparently modern-secured network. (Intelligence and National Security Alliance, 2011).
Cyberattacks impact on businesses can be measured by their economic impact and the cost that they generate. According to a CISCO research that involved more than 3600 organizations across 26 countries, more than 53% of all attacks caused financial damages of more than 500,000$/incident (where 8% of the incidents generating costs of over 5 million $/incident), including, but not limited to, revenue lost, customers, opportunities and out-of-pocket costs (CISCO, 2018).

Furthermore, security professionals, in their efforts to protect their organizations face many roadblocks. For both public and private sector, the main constraints when managing security issues are: financial constraints, compatibility issues regarding legacy systems that are still in use and lack of trained personnel. The same CISCO report compares these main three constraints over a period of three years – 2015-2017 (Figure 1).
The research results highlight that budget constrains have represented the main obstacle for more than 3600 organizations, in their attempt to prevent or correct cybersecurity issues. On the other hand, while budget constrain related barriers decreased over the years, another issue is rising (by approximately 10 % in only 3 years) and challenges modern organisations and the security of cyberspace – lack of trained personnel in dealing with modern cybersecurity protocols and threats.

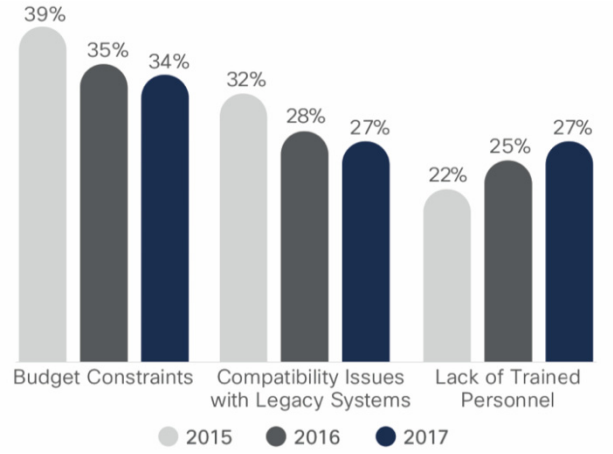

Fig. no. 1 The main constrains public and private organizations face when dealing with cybersecurity issues

Source: Cisco Annual Security Report, 2018, available at: https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf

Thus, the emerging trend regarding the lack of specialized human resources is also highlighted by different studies. Moore et al (2016) conducted an interview on approximately 40 organizations, discussing mainly with executives responsible for cybersecurity, like Chief Information Security Officers (CISOs) or Chief Information Officers (CIOs), from different sectors like healthcare, financial, retail and government. A total of 78% of the respondents were from the US, while the difference had other international headquarters. The interview was structured in multiple sets of questions, focused on three main areas: identifying threats, prioritizing and managing preventive and corrective actions and decision-making process for cybersecurity investments.
The main results revealed small differences between certain industry and governmental sectors, but remarked, for all the analysed sectors, a growing trend that organisations are facing: finding qualified cybersecurity professionals tends, in general, to be much more challenging that finding the necessary financial resources to support cybersecurity.
At a first analysis, a decrease of budget constrains over the years should result in more financial resources that can be invested in multiple activities regarding cybersecurity. According to quality management principles and CAPA[1] programs, one of the most

[1] corrective action/preventive action programs focus on the investigation and solving of problems, by identifying causes, taking corrective actions and preventing recurrence of the root causes

important actions that need to be financed are the preventive actions, that are implemented prior to the occurrence of a cyberattack, representing proactive tools that involve monitoring a system's effectiveness in terms of data protection.
Thus, in this context, a very important preventive action that a company or an organization can include in its quality management program involves training activities in order to have specialized personnel that can efficiently manage the 5 core functions of an effective cybersecurity plan - identify, protect, detect, respond and recover (Pelton and Singh, 2015).
So, a main hypothesis is that organizations define their cybersecurity strategy based on preventive actions, that can be implemented and monitored by trained personnel. Therefore, the costs associated with cybersecurity trainings for the employees responsible with security in this domain are considered investment costs, that result in long term benefits for the organization. In other words, taking into consideration the actual costs that a cyberattack can generate, including a training budget in the organisation's financial planning can save a lot of money in terms of corrective actions, when an actual threat becomes an attack.
But, when confronting different research results, the correlation between the 2 trends does not meet the above hypothesis. Thus, a decrease of budget constraints correlated with an increase in finding specialized cybersecurity professionals, means that organizations, despite of the fact that they are aware of the lack of specialized personnel, do not redirect financial resources in cybersecurity trainings and specialization programs. This fact can be determined by multiple causes like: the sophistication of cyber threats, as their complexity evolve faster than the personnel can be trained, IT specialists are not interested in this specialization as access to critical data comes with additional risks, insufficient training programs and educational resources that can be accessed by cybersecurity experts.
Thus, considering the way humans, companies, government and technologies interact, security education is desirable to strengthen the knowledge of all involved parties, starting with government officials, big IT corporations and citizens with regard to cybersecurity issues (Li & Liao, 2018), in this sense, specialized educational programs having an important role.

2. The need of Cybersecurity educational programs as a main instrument in preventing cyberattacks

Cybersecurity educational programs should represent a valuable resource for a nation, a company or an international organization. According to different studies, graduates of computer science programs should have taken at least one cybersecurity course over the years and more and more universities are introducing new courses regarding cyberspace security in order to meet society's emerging needs regarding data protection.
But, in this context, where technology and the internet evolve with the speed of light, "at least one cybersecurity course" can be consider enough to form a cybersecurity specialist?
Taking into consideration the wide spread of cyberthreats and the multiple and complex typologies of cyberattacks, cybersecurity officers should be well more than well trained in order to be able to working with and protect national security information or back databases.
In order to better understand the complexity of this domain, a diagram representing the main cyberattack types is provided below (Figure 2). Thus, one can understand that a well-built cybersecurity educational program involves resources from multiple domains and, in order to keep in touch with technology's fast evolution, research and development activities and implicitly their associated costs must be assumed.

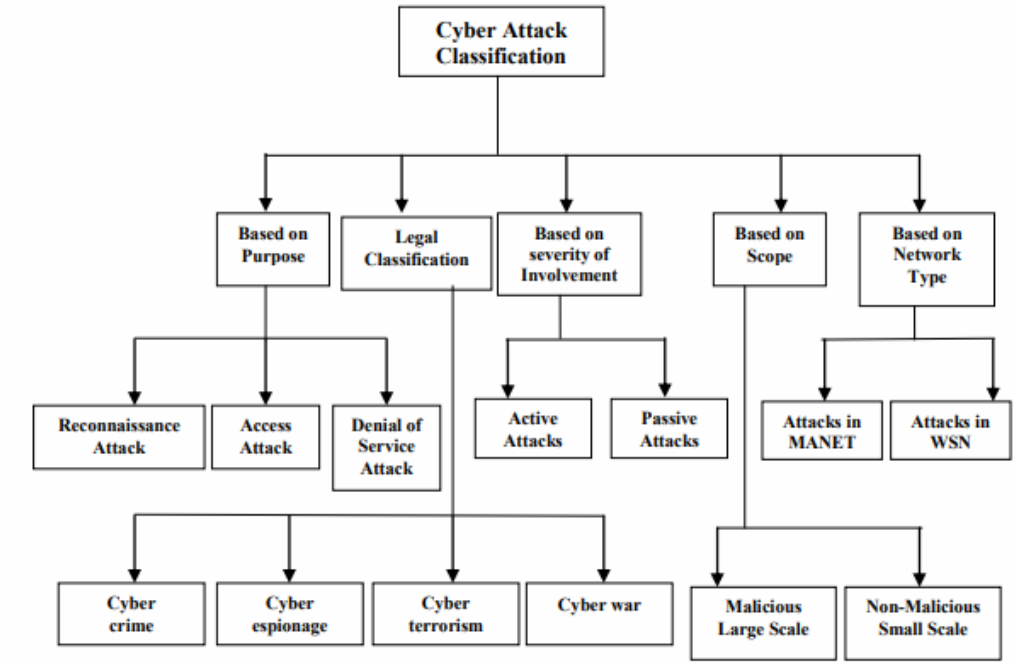

Fig. no. 2 Cyberattack classification diagram
Source: Uma and Padmavathi, 2013

Information security is still a relatively new profession (and its branding as cybersecurity is even more recent), which means there is still some debate about the level of professionalism within it (Furnell et al, 2017). Therefore, governments or companies are still investing more in corrective actions than in preventive strategies. The educational resource has been recently considered as a main priority by different national cybersecurity strategies, or by international organizations like NATO.

The academic environment and the training industry should have a more important role in developing this domain and in building cybersecurity strategies. Skills-dominant approaches and delivering authorized trainings to students or workers represent main resources that form professionals in data security. Even if educational costs or training fees can cost organizations more than expected, there are more benefits realized from making those expenditures. Some studies (Böhme, 2010) highlight that there is a baseline level of security driven by preventive efforts for risk mitigation, but, at some point, the costs level out, reducing external breaches and making organizations realize that it would cost much more to correct than to prevent.

When talking about cybersecurity educational programs as a main instrument in preventing cyberattacks, the main focus areas (education, training and research) and their main determinant factors should result in identifying improvement strategies (Figure 3).

Fig. no. 3 Conceptual model – The relationship between the key elements of cybersecurity education
Source: own research

Thus, a set of recommendations and good practices have resulted from the analysed researches:

- local industries (mainly IT&C companies or the banking sector) should be involved in supporting educational initiatives, such as paid internships and trainers provision;
- government structures should and the academic environment should work in a close relationship, by promoting temporal professional exchange of information and good practices in order to promote security's role in cyberspace;
- international organisations and partners can be a good source of information in this field;
- availability of more virtual training environments in order to connect more specialists from around the world;
- building quality research upon existing capabilities and structure, including experienced investigators, funding, research centres and feasible projects.

Conclusions

Beside the value added to multiple global economy sectors and to the modern society itself, cyberspace can generate a number of risks and vulnerabilities for both public and private sector of a country, even with regional or global consequences.

Thus, the notion of cybersecurity represents a main topic for multiple international organizations that constantly analyse potential threats in order to develop security strategies against cyberattacks. In this context, skills associated with professionals working in this field tend to be more complex than IT-specific ones. Adding complexity in assessing a particular qualification requirement is the risk associated with security operations, security professionals aiming to have a higher level of access to critical data.

Therefore, in order for an organisation, both public or private, to benefit from the support of specialized personnel in preventing cybersecurity breaches, a sustainable approach must be adopted and specialists must act as risk advisors, by thinking in terms of the cost-benefit aspects of cybersecurity investments.

Besides investing in preventive technologies that aim to avoid the negative effects of cybersecurity breaches, organizations must invest first in educating and training their own personnel, so that these technologies can be used in an efficient manner and some of the cybersecurity risks associated with potential future breaches can be transferred in the preventive action zone.

References

Böhme, R., 2010. *Security Metrics and Security Investment Models*. Berkeley: International Computer Science Institute.

Campbell, K., et al, 2003. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, 11(3), pp.431-448.

CISCO, 2018. *2018 Cisco Annual Security Report*, [pdf] Available at: <https://www.cisco.com/c/ dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf> [Accessed 20 February 2019].

Furnell, et al., 2017. Can't get the staff? The growing need for cyber-security skills. *Computer Fraud & Security*, 1, pp. 5-10.

Gordon, L.A., Loeb, M.P., Zhou, L., 2011. The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, 19(1), pp.33-56.

Intelligence and National Security Alliance, 2011. *Cyber Intelligence: Setting the Landscape for an Emerging Discipline*. [pdf] Available at: <https://www.insaonline.org/wp-content/uploads/2017/04/INSA_CyberIntel_WP.pdf> [Accessed 20 February 2019].

Li, H., Gyun No, W., Wang, T., 2018. SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, 30, pp.40–55.

Moore, T., Dynes, S. and Chang, F.R., 2016. *Identifying how firms manage cybersecurity investment*. Berkeley: University of California.

Pelton, N.J., Singh, B.I., 2015. *Digital Defense, A Cybersecurity Primer*, Springer.

Radziwill, N., Benton, M., 2017. Cybersecurity Cost of Quality: Managing the Costs of Cybersecurity Risk Management. *Software Quality Professional*, 19, pp.16-35.

Uma, M., Padmavathi, G., 2013. A Survey on Various Cyber Attacks and Their Classification. *International Journal of Network Security*, 15(5), pp.390-396.