THE HUMAN FACTOR IN CYBER SECURITY

ISABEL MARGARIDA AFONSO DA SILVA BAPTISTA

Summary

Dissertation for the Master's Degree in Information Security and Law in Cyberspace

Thesis Advisor: Professor Doutor Carlos Ribeiro

Second Reader: Professor Doutor Pedro Veiga

Lisbon, 31 october de 2017

Rapid evolution in information and communication technology (ICT) have had a profound effect on contemporary society. Today, individuals, organizations and the State need the Internet and ICT in general to perform daily tasks, which means that society and individuals are increasingly dependent on technology.

Individuals rely on ICT in their daily lives, resulting in an almost omnipresent adoption of digital technology. Referring only to a few examples, the individual uses information systems to perform his professional functions, play on games consoles and watch movies on tablets for entertainment, use online resources to study, make purchases on the internet, interact and make inquiries on the internet through smartphones, check the number of calories consumed and the number of hours slept through sensors placed on the wrists, among many other activities.

Information systems are thus fundamental to the success of the Information Society - a globalized society, where sharing, simple and easy access to information is predominant.

The constant development of new threats (predominantly malware), the high numbers of Internet attacks (such as data theft of data, contact lists or banking information), identity theft or extortion (the most common of which is ransomware), require citizens to become increasingly aware of the importance of protecting their information and to become experienced and aware of available means of protection.

Apathy, ignorance or non-awareness of security, as well as technological illiteracy, are the greatest threats to information systems. It is now known that the best way to achieve a significant and lasting improvement in information security is not only through technical solutions, but also through increased awareness and appropriate behaviour by individuals in the use of information systems. What common digital security practices should be continue to be ignored by most individuals, including young people who are born and raised alongside technology, endangering not only the security of their data and information (including their privacy), but of all those around them.

However, the extent of the consequences of these safety practices also depends on the clear and complete understanding of the risks to which the information may be subject. Awareness raising is the starting point for the development of a successful cyber-citizen empowerment program.

The critical role of consciousness in the organizational environment has been widely advocated in the Information Warranty literature (Hewitt, 2013). Organizations use massive information systems, linked to internal networks and the internet, inside and outside the perimeter of the organization's own infrastructure. Simply put, with increased connectivity, the risk of attacking organizations' networks is also increasing.

In addressing the issue of information security, three issues influence the need for a citizens' empowerment program for cybersecurity, where confidentiality, integrity and availability are highlighted. It has been long acknowledged that information is secure when these three

properties are present. As addressing the two components of risk - threats and vulnerabilities is one of the primary objectives of this work, the proposed training programs will focus on the risk reduction component, namely the protection of confidentiality, integrity and/or availability of organizations' information.

Taking into account the reality described it is considered fundamental to contribute to awareness raising of cybersecurity issues. Therefore, the work developed within the scope of this master's thesis focuses on the design and development of a cybersecurity citizenship training program, namely in the development of awareness, training and evaluation techniques for best practices in using technological resources.

In preparation of this research, several prominent cybersecurity training programs were observed and analysed, namely those developed by other National Cyber Security Centres or organizations related to awareness raising of these issues. The National Cybersecurity Centre in Portugal (CNCS) considers that it is essential to support the protection of the confidentiality, integrity and availability of information from State agencies and Critical Infrastructures (CI), ensuring that each individual involved understands its responsibilities within the organization and in the information society itself, and is sufficiently prepared to perform its functions safely.

In cybersecurity, users are often referred to as "*the weakest link*" (K. & W., 2014, p.361). The latest report by IBM Security and Ponemon Institute (IBM Security & Ponemon Institute, 2017) estimates that the cost of security breach incidents in organizations in the United States has increased. Of these incidents, 31% were caused by employees' negligence.

User risk behaviours are responsible for a substantial part of all cybersecurity attacks and represent a considerable cause in the increase of successful attacks (Paganini, 2013). In this regard, Paganini (2013) points out that "*new online business opportunities, mobile platforms, cloud storage and social networks are considered privileged areas of success for users not aware of possible cybersecurity threats*" (Paganini , 2013).

On the other hand, some types of risk behaviour also results in security breaches that, by not materializing cybersecurity attacks *de facto*, result in the creation of vulnerability conditions that increase the technological exposure to such attacks. Examples of such behaviours might be not to log-off on open sessions from application accounts, share login credentials, fill out forms with personal information without knowing if the source is trusted (Paganini, 2013), view phishing emails, not reporting stolen devices (Ranger , 2014), being unable to judge whether one may be a victim of social engineering (defined as "*the art of gaining confidence or acceptance to persuade someone to provide information or to take action to benefit the attacker*" (Nakamura & Geus, 2007), using short or unsafe passwords (Athitakis, 2014), or making bad decisions in web browsing, such as clicking advertising windows (Blue, 2014), which can be used to spread malware.

Typically, the individuals more exposed to risk are the least informed ones, innocent, and poorly aware of the basic principles of cybersecurity, which we consider relevant to point

out since "*many external attacks - more than 60% - are directed to employees via social engineering "Which" ... exploit activities through e-mail and social networks*"(Caldwell, 2013).

Employees can be considered as the organization's first line of defence against cybercrime and cybersecurity incidents in general, however, they are also the highest security risk and the most common cause of data breach (Devaney, 2012). In fact, passive attitudes towards cybersecurity are not only seen in individuals or employees with less responsibilities, but also in managers or senior managers with high responsibilities within their organizations. Many leaders believe that cybersecurity is an ICT-related problem, but it is primarily their responsibility the creation or enhancement of a security culture in their organizations. This thought is defended by Posthumus and von Solms (Posthumus, 2004: 646), who assert that "*governance of information security is a complex issue that requires the commitment of everyone in the organization to protect valuable information assets from the company*".

It is a fact that organizations may not be able to eliminate the risk, but if decision makers are trained and aware of cybersecurity issues, they are more likely to manage risk and make decisions about the investment needed to mitigate that same risk. In this sense, organizations, in addition to infusing technology into their business models, must also follow the digital evolution so that they can consider the inclusion of cybersecurity measures as a differentiating factor of success and risk reduction.

Considering that cybersecurity incidents continue to increase in frequency and sophistication, organizations should try to understand where data security breaches typically occur. The report by IBM Security and Ponemon Institute (IBM Security & Ponemon Institute, 2017) found that the average overall cost of a data security breach is $3.62 million, a decrease of 10% over 2016 (US $ 4 million). In this study, overall costs have decreased, but in many regions they actually increased. This report also reveals that incident response, cryptography and education (training) were the factors with the greatest impact on reducing the costs of data breaches.

A geographical significance can be noted in the training programs for existing citizens. Each program analysed, from which a literature review was conducted, revealed specific characteristics of their country of origin. These contributed to (and were a source of inspiration for) the training program objective of this thesis. In order to have some indeapth on the national reality, national projects were also closely analysed, with the objective of not overlapping the target public. Also the data of the Annual Homeland Security Report - 2016 (RASI) was analysed, and it was concluded that Portugal registered a growth of ransomware and a stabilization of the use of virtual currencies. This report suggests a greater investment in awareness raising, particularly in matters that impact on computer crime. A career in cybersecurity requires relevant and often specific skills. However, this specificity has not yet any reflex in the formal identification of the relevant competences, leading to the possibility of finding an immense variety of training and teaching courses on the market, typically referred to as

retraining or retraining courses. Choosing the appropriate course/training is a challenge for those seeking qualifications or preparedness to enter or developing a career in cybersecurity.

It is imperative that States respond effectively to the challenges posed to them by the evolution and dependence of today's societies on information and the need to ensure the security and availability of critical services that underpin these same societies and information, directly or indirectly, in infrastructures and technological processes.

States and, above all, organizations play a key role in the development of societies and the promotion of technological innovation, based on the need for citizens to have skills and awareness in order to keep up with developments in technology. The signs of political recognition that cybersecurity is today strategically relevant, as seen in the strategic options enunciated by the President of the European Commission, Jean-Claude Juncker. The reference to the lack of citizens' awareness and knowledge of cybersecurity matters, reinforce confidence that the investment in the creation of a training program in cybersecurity will be welcomed by the citizens.

A cyber-security training program is nothing more than a cyber-hygiene program that will contribute, among other things, to reduce the number of cybersecurity incidents that occur due to lack of citizens' awareness of these issues. In this sense, an enticing way of informing citizens and workers about malicious activities occurring in cyberspace and targeting the organizations where they work is to invite them to participate in a cybersecurity training program.

E-Learning is a commonly used and widespread learning method. These systems are complex and aim to ensure student satisfaction and maintenance a good image of the learning process. There is now clear evidence that innovative educational technologies, such as E-Learning, offer unprecedented opportunities for students, teachers, and other professionals who want to acquire, develop and maintain essential skills and knowledge. In addition, the latest E-Learning platforms have modified the idea of distance education, increasing the possibilities of teaching/training for those who consider E-Learning an option. Also, companies took advantage of the benefits of this solution early on, stimulating the training and awareness of their workers.

Digital technology has undergone rapid expansion and dispersion, making MOOC (Massive Open Online Courses) a form of mass distribution of knowledge, transforming training and education into a more open, equitable and flexible logic driven solution. In this way, MOOCs are online courses designed and created for a large number of participants, which allow anyone to access them anywhere (subject to the need for internet connection) and that are free and open to all without restrictions.

Cybersecurity incidents do not discriminate organizations or citizens, occurring in vulnerable information systems whether they belong to a large organization, to a small business or to a common user. Cybersecurity should thus be a shared responsibility and all citizens and workers should have a role to play. The Cybersecurity Training Program that we intend to

achieve based on the principles we develop in the thesis, as well as its implementation, provide suggestions for resources for all segments of society. In this sense, a table of Competences in Cybersecurity is presented, aligning segments of society (professional function), needs and level of cybersecurity competencies to be acquired.

Table 1 - Dimensions in Cybersecurity Table

Dimensions of cybersecurity

	Organizational	Economic Management	Legal	Technical	Behavior
Senior Management	H	M	M	L	H
Intermediate Management	M	H	M	L	H
Technical Manager (ICT)	L	L	L	H	H
Functional Manager (financial area, human resources, procurement, logistics, ...)	L	M	H	M	H
Worker/ Citizen			L	L	M

Caption: A - High, M - Medium, B - Low

The human factor, in particular behaviour, is fundamental and cross-cutting, and should be taken into account in cybersecurity. If certain behaviours are not part of the organization's culture and are not regarded as central in the prevention of internal or external incidents, then there will never be enough Information Systems to protect the user from potential threats. Educate, train and sensitize employees and citizens to appropriate behaviours for an organizational culture of cybersecurity is the basis for strengthening organizations. All segments of society (professional functions) need awareness, therefore the cybersecurity training program that we propose to develop is focused on the cybersecurity competencies that any worker or citizen should possess.

This thesis therefore proposes the development of an E-Learning course, using the MOOC methodology, which fosters a cross-consciousness of society, citizens and workers in general (a need highlighted in the table). In order for this course to reach as many citizens as possible, it will have to be widely publicized on the various government sites, on the intranets of as many State bodies as possible, and on public service sites targeting the citizen.

This citizen-training program in cybersecurity should be accompanied by a communication plan that includes a variety of means, such as information leaflets and flyers, posters and merchandising, videos, posts on social networks of organizations (GNS and CNCS in particular), with simple, direct and understandable messages to the general public. In order to maintain and constantly update the contents of this cybersecurity citizen-training program, it is

proposed that an annual internal assessment should be developed, with input from the RASI data, the main trends in cybersecurity, the statistical evolution of incidents and threats, ENISA reports on lessons learned and feedback from users and organizations communicated through the course evaluation forms.

During the development phase of the author's thesis and professional experience, the need for greater investment by organizations and the Public Administration in Personware Management was identified. In this context, we identify Personware as the human resources of an organization that allow the proper functioning of hardware and software - workers with roles in IT.

Today's world is full of technological challenges, leading to a demand for human resources with specific skills and capabilities. Fortunately, organizations have individuals among their staff who also aim the adaptation of their profile to the needs of the market. In the process of worker growth within an organization, there is inherent recognition of the competencies of learning potential, behaviours and training needs, as well as anticipation of the requirements of the organization. Organizations that promote the professional development of their workers through an adequate and adjusted career plan that includes professional training is also contributing to the achievement of its organizational objectives.

In this sense, organizations must develop a career plan per employee that includes, among others, a description of roles and responsibilities, commonly defined as a job description, and the evaluation of the employee in the function he performs. Personware management always starts with the employee and how he fits into the organization. Personware, unlike software and hardware, is a self-assessment mechanism, which should include the description of the function developed by the worker within the organization, the position’s roles and responsibilities and the skills and education necessary to perform these duties.

The investigation and subsequent implementation of a Personware Management model in Cybersecurity is therefore proposed as an element for future studies, which must start from a framework identifying the relevant competencies by role and intersect them with a matrix that is the result of the intersection of the responsibilities of the workers and their evaluation in the organization, with the correspondent self-assessment.

References

Athitakis, M. (Junho de 2014). *Data security: Keep a lid on it.* Obtido de Now associations: https://associationsnow.com/2014/06/data-security-keep-lid/

Blue, V. (2014). *Hacked: The six most common ways non-tech people fall victim.* Obtido de zdnet: http://www.zdnet.com/pictures/hacked-the-six-most-common-ways-non-tech-people-fall-victim/7/#photo

Caldwell, T. (12 de February de 2013). *Risky business: why security awareness is crucial for employees.* Obtido de The Guardian: https://www.theguardian.com/media-network/media-network-blog/2013/feb/12/business-cyber-security-risks-employees

Devaney, T. &. (2012). *Forbes*. Obtido de 5 Ways Small Businesses Can Protect Against Cybercrime: http://www.forbes.com/sites/capitalonespark/2012/12/17/5-ways-smallbusinesses-can-protect-against-cybercrime/

Hewitt, C. (2013, January). *For Privacy and Security, Use public Keys Everywhere.* Palo Alto, CA.

IBM Security & Ponemon Institute. (2017). *2017 Cost of Data Breach Study.* Obtido de https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN

K., R., & W., G. (2014). *The curious incidence of security breaches by knowledgeable employees and the pivotal role a of security culture.* Obtido de K., R., & W., G. (2014). The curious incidence of security breaches by knowledgeable employees and the pivotal role a of security culture.

Nakamura, E. T., & Geus, P. L. (2007). *Segurança em redes cooperativos.* Obtido de https://books.google.pt/books?hl=pt-PT&lr=&id=AamSIJuLc34C&oi=fnd&pg=PA11&dq=Nakamura,+E.+T.,+%26+Geus,+P.+L.+(2007+).+Seguran%C3%A7a+em+redes+cooperativos.+S%C3%A3o+Paulo:+Novatec.&ots=Y0AkjefpP2&sig=8P_lr3i8S4R1kYFAac0A8B8sMBo&redir_esc=y#v=onepage&q&f=

Paganini, P. (2013). *the importance of security requirements in designs of SCADA systems (PenTest auditing and standards 2012:06).*

Posthumus, S. &. (December de 2004). *Computers & Security.* Obtido de A framework for the governance of information security: http://dx.doi.org/10.1016/j.cose.2004.10.006

Ranger, S. (2014). *NATO Updates Policy:Offers Members Article 5 Protection Against Cyber Attacks.* Obtido de http://www.atlanticcouncil.org/blogs/natosource/nato-updates-policy-offers-members-article-5-protection-against-cyber-attacks

Table of Contents