INFORMATION SECURITY AWARENESS IN CONTEMPORARY ORGANIZATIONS – CHALLENGES AND SOLUTIONS

Assoc. Prof. Popescul D. PhD
"Alexandru Ioan Cuza" University, Iași, Romania

rdaniela@uaic.ro

Abstract: *Nowadays, we are witnessing a constant increase of cybersecurity-related threats and dangers. New trends such as monetization of attacks, their virulent propagation through social media channels, the abusive collection of data through interconnected smart things, with little concern for the privacy of the user, are expressed by the important security solutions providers around the world. In addition, the academic literature presents numerous real and proof-of-concept attacks and security problems that have a considerable impact in various domains. On the other side of the story, the organizations usually ignore privacy and security concerns, and there is a very low level of awareness regarding these issues. The need for related training programmes and educational curricula in this area remains almost unanswered. In this context, the paper analyses the security measures applied in contemporary organizations with the purpose of raising employees' cybersecurity awareness and discusses their effectiveness, using a sample of 25 small and medium Romanian enterprises, with the intention to identify the current and to propose future viable solutions for raising awareness and inducing ethical behaviour among employees.*

Keywords: INFORMATION SECURITY AWARENESS, INSIDER THREATS, SECURITY TRAINING

1. Introduction

Today, the subject of information security (IS) has become very complex. Various types of tacit and explicit knowledge, from traditional fields as information and communication technologies (ICT), but also from business administration, human resources, psychology, finance and legislation, mix and mingle in this organizational area, transforming it in a very provocative one. The technical expertise of network administrators and other ICT specialists is no longer enough for protecting an organization, due to the complexity of human actions, organizational processes and regulatory policies associated with IS. Information assets' fragility and vulnerability increases steadily, as digital information can be easily copied, destroyed, or forged, as shown in [1] [2] [3]. New and ingenious threats occur in cyberspace every year, causing security breaches that determine financial and productivity losses, and forcing organizations to respond with updated security measures. In this context, is of utmost importance for organizations to be aware of the risks associated with the use of ICT in business processes and to positively address this issue by training employees in such a way that they understand the types of threats, risks and vulnerabilities specific to digital work environments and are able to apply appropriate security measures.

2. Literature review

The need for education in IS field has constantly been affirmed by academia, important security organizations [1] [4] [3] [5], and cybersecurity solutions providers [6]. In [7], creation of IS competencies is seen as a social and economic need, a critical cross-field outcome, a way to narrow the evident "information security gap" in universities and businesses. In order to prevent "a divide into Digital Elites and Analog Illiterates with dramatic consequences for societies", in [8] and [9], cybersecurity education is considered an important step in assuring a sustainable development, a part of lifelong learning processes. Various solutions for active learning, with practical outcomes and useful hands-on experiences are proposed, e.g. gamification [10] [11], Web 3.0 ontologies [12] or cloud computing platforms that offer teaching staff and students (on-demand, elastic, dedicated, isolated, (virtually) unlimited, and easily configurable virtual machines [13]. Also, [14] highlights the need to ensure that employees are informed and aware of their obligations toward information security in organizations.

Our research question, based on the above formulated elements, is related to the extent in which users are aware of the IS threats and vulnerabilities in the organizations they work in, and what's their perception regarding the important security measures adopted and needed in organizations.

3. Methodology

The study was conducted in the framework of an elective course of *Information Security* taught at the Faculty of Economics and Business Administration of Alexandru Ioan Cuza University, Iasi, Romania to a group of up to 50 students enrolled in a non-ICT undergraduate programme. None of the students had prior experience in IS before the course and none of them attended any form of formal education in the field. The topics covered in the course are IS challenges brought about by computers and the Internet, importance of protecting information assets, key concepts in IS (e.g. information assets, risks, vulnerabilities, threats, confidentiality, integrity, availability, authentication, authorization), information classification, physical, logical and administrative access control measures, information security policies, data storage, backup and recovery, personnel security, encryption, steganography, systems security and some elements of network security, ethical and legal issues (software piracy, code of ethics, privacy law, copyright). After discussing the threats and vulnerabilities that may affect an organisation (based on ENISA framework) and the security measures recommended for a proper protection of data, information and knowledge during 4 meetings of 4 hours each, the students were asked to identify the most important threats and vulnerabilities recorded at their working place/in other known organisation, to present the security measures adopted by the organisation and to propose some new measures which they consider important for a better protection of information assets. Students were requested not to disclose any information or data that could possibly lead to the identification of the organisation. For this paper, the most comprehensive 25 reports were selected and analysed, with the intention to identify the most frequent threats and vulnerabilities the students became aware of after the class, the security measures they consider important, and their recommendations about possible improvements in IS in their immediate proximity.

4. Results and discussion

The most frequent threats identified by the amateur analysts can be categorized in insider threats (attacks and errors), malware, physical damage, and identity theft. Some example for insider threats, in students' own words, are the following:

"An IT employee, whose name was on the dismissal list, blocked the entire billing cycle, with the intention to persuade the manager in changing his mind and keep him in the company"

"Important documents were stolen and sold to interested third parties, due to the lack of passwords for each file"

"As the same laptop was used by many employees without any user accounts, so it happened that an employee deleted data of the others"

"Errors occurred in payrolls and order reports, caused by the insufficient ICT competencies of some older employees, who had problems in understanding the accounting software"

"Folders and files were deleted by mistake"

"A user did not check the ERP software' HASP protection key, which was not correctly entered into the computer. The employee worked on a demo version of the program, nothing was saved and the work had to be started over"

"By mistake, a folder with important documents was thrown away during a general cleaning period"

"During a faulty update of the accounting software, all existing data were deleted"

Also, disclosure of confidential information, as a consequence of missing non-disclosure agreements (NDAs), improper procedures and absence of IS trainings, and a laptop theft were noticed.

In many organisations, computer viruses caused *„system malfunctions, data processing delays and financial losses"*. In some cases, reinstallation of the operating system was necessary, in one organisation "*obscene messages were displayed in browser (title bar)"*. In a case, "*a fake antivirus software deceived an employee and, after he accepted to install it, the mouse and keyboard were blocked and the computer was repeatedly shut down"*. Other three cases of phishing were noticed, and four cases of ransomware – in one of those, the manager paid the reward for the decryption of organisational data, as no backup was available.

The physical damages were frequent enough. In two cases, *"a heavy rain damaged documents, cables, and computers"*. In another organisation, "*flood caused by a broken water pipe on the 1st floor deteriorated many documents and computers in the ground floor"*. Malfunctions in the power supply network are among the most important threats mentioned, *"because not all computers are protected by UPSs and information is lost"*. Due to the obsolete infrastructure, failures of the power supply are very common. They have a destructive effect on computer components, especially CPUs and hard drives. In some cases, data integrity was affected. In one enterprise, "*the accountant's laptop broke up due to a mechanical shock, and records for an entire month were lost*".

Regarding the financial identity theft, "*there was an attempt to clone a card (manager's card), from Peru"*, and a successful money withdrawal from one company's account. Also, a situation in which usernames and passwords were stolen by a keylogger was identified.

Vulnerabilities observed by the students were related to:

- passwords: no, default or weak passwords, *"passwords placed on sticky notes and visible to any person who enters the room"*, *"access codes, passwords and keys are not changed after an employee leaves the organization for good"*;
- weak ISPs and procedures: software installation permitted to any employee; unrestricted access to Internet, "*making employees feel free to play games, watch online TV, use social media pages in their personal interest"*, unsecured portable computers (laptops), vulnerable to loss, theft and unauthorized data access, no backup policies/procedures, too lax BYOD (Bring Your Own Device) policies, "*USB sticks are used outside the organization, in unsecured computers, and then they become a malware access point in the organization's network"*; or, in the worst case, *"no policies/procedures at all"*;
- unaware, uninformed employees, due to the lack of proper ICT and IS knowledge and training: "*employees cannot distinguish between normal and spam messages"*, *"personal data are transmitted on unsecured channels"*;
- other vulnerabilities: untrustworthy employees, due to "*faulty recruiting and selection processes"*, unwary guardians, tired employees, dusty or humid environment, old computers etc.

Regarded the security measures in place, students mentioned firstly the obvious ones. The equipment *("electric and non-electric fire extinguishers"*), materials and plans for fire intervention were noticed in all the organisations. Some organisations use gas detectors in archive and computer rooms, but only in one case, *"a quarterly training on fire extinguishing and work safety"* was mentioned. The usual physical access control measures observed were: fenced yard, keys (with some mentions that "*for spaces like organizations' archive or server room the key is doubled by a code"*), special attention to the main keys, video interphone, magnetic cards for employees (unique ID for each employee). In a case, the analyst mentioned that *"computer rooms are placed at a safe enough distance to production unit, because computers need to be protected from wastes generated by the fabrication of cotton clothing (especially lint, dust etc.)"*. Other noticed that *"the access of staff in certain areas of the unit is limited, based on a badge"*, and *"for some operations two people are needed because special information assets-related activities are done only in the presence of an authorized person"*. Many noticed that servers are located in special rooms, with restricted access, that the computer rooms have windows with bars, they are placed under video surveillance, and *"at night the buildings are secured by alarm systems"*.

Hardware protection measures noticed during the analysis referred to "*careful provision of spare parts and supplies for the computers"* and "*the periodical cleaning of the dust inside the CPUs"*. Students noticed that the organisations use licensed and updated software, antivirus software (but usually the basic, free version), they launch periodical scans for threats and they use firewalls for scanning the Internet traffic.

Identified backup procedures were diverse: weekly backup for accounting and financial data (with USB sticks and external hard disks as the most used supports), digital copies for the most important documents on paper (contracts, for example), periodic backups, "*with priority for data of the highest importance, such as: employee payroll, employee records (record of employment contracts and seniority). In one company, periodic simulation of restoration from copies are made, together with logging of problematic events and defects, where possible, and permanent monitoring of critical equipment"*. In the event of maintenance or repair of the ICT equipment, a student noticed that "*all data is saved on external drives in order to avoid the access of unauthorized third parties, thus ensuring their confidentiality and integrity"*.

Passwords are used in various ways: passwords per employee and device, known by the user only – if a replacement is needed in an exceptional situation, a special authorization is issued, signed by an authorized person; complex password per device; username and password for financial and accounting software and for the wireless router. In three organisations, *"passwords are changed frequently (1 to 3 months) and every time after an employee leaves the organisation"*. In one case, *"digital fingerprint readers on manager's and accountant's laptops"* were signalled.

Correct document storage procedures were noticed in the majority of organisations. For example, in one company *"important documents are stored in cabinets equipped with locks, and only Human Resources and Financial Accounting departments' managers have the keys"*. In another, *"the documents are moved weekly in special boxes, which are then stored in a locked room"*. Most documents are properly archived – *"tagged, dated, placed in shelves on the edges of which the company name is written and moved in a separate room"*.

Digital signatures are largely identified in the analysed organisations, due to the fact that is mandatory for the accounting experts to submit the online statements on the website of the National Agency for Fiscal Administration (ANAF), using an electronic signature obtained through a digital certificate. It can also sign electronically and contracts, tax invoices, tax returns, reports and balance sheets. These electronically signed documents have the same legal value as paper documents signed and stamped. Moreover, being an electronically signed document with a digital certificate, they are much more difficult to fake than a stamp or a

hand signature. The electronic signature uses two security tokens and its PIN and cannot be forged, making it much safer than the handwritten signature. At the same time, the use of electronic documents is faster, cheaper and more efficient.

In the sphere of employees related measures, *"a careful personnel selection process was mentioned twice"*. In many organisation, at least a CV/resume and a verified recommendation from the latest workplace were requested. In one report was mentioned that, *"when elaborating the job description contract, security-related tasks are not skipped. Precisely to reduce the risks of human error, theft, fraud or abuse of trust, the implementation of security responsibilities starts from the recruitment stage. Personnel is also closely monitored*". Other measures say that *"employees must have the necessary training for the job and comply with the internal regulations of the organisation and their job description"*; that *"they are required to keep important information confidential (in some cases through NDAs) and are not allowed to upload confidential data and information on external websites"*. When an employee leaves the job, for various reasons, *"he or she has to give back the mobile phone and the keys"*. In one organisation, the manager kept "*the workload in reasonable limits, as a way to help employees in working carefully, correctly and in an organized manner, providing accounting data on time and with a high level of integrity (as accurate as possible, in his words)"*. In another, ISPs are presented to every new employee, for the safe use of computing systems.

Only one mention was made about a specific training on ISP, probably on GDPR application. In the same enterprise, *"the manager periodically informs the personnel about malware, phishing, spam etc. The website uses a secured connection through https, digital certificate, restricted access at the administration page. In the organization there is a person in charge of maintenance of equipment and software and this specialist is responsible for training the personnel in the use of software. The loyalty of the employees is an important focus, in order to avoid the threats. Training occurs usually when new equipment or software is bought and installed. Registered threats are described and communicated to all the employees, they are also entered in a special register. The exchange of information and software between the different institutions with which there are collaborative relationships is monitored; the director of the organisation is following these exchanges to comply with the legislation in force; procedures and standards shall be established to protect data and information in transit which are initiated in Partnership Agreements."*

Other measures noted by analysts are computers' stand-by mode after a 20-minute period of inactivity, document shredders, supervised third-party access to computers.

The students came with recommendation for improvement of the IS in the analysed organisation, extracted from the course materials/inspired by discussions during the classes:

Proposed measures for access controls referred to "the *redefinition of access rights, especially for physical access in special-purpose rooms and offices (archive, server room etc.). The number of authorized persons in these special spaces should be reduced to a minimum value*", *"digital fingerprint at the main entrance and other important rooms"*, *"no more default passwords for devices (routers or surveillance systems) and also for software"*, wireless surveillance system, movement sensors. Regarding the access to documents, *"a closed computer system that prevents the extraction / copying of documents, folders or any other confidential information from the computer and, when such an attempt occurs, the administrator is alerted"* was considered a good idea.

In many cases, "*the upgrade of the current antivirus to a better version, with anti-phishing, anti-ransomware, anti-spam protection"* was suggested.

In the personnel security area, following recommendations were made:

"Security courses regularly attended by employees, because everyone needs to know how to recognize a phishing message, know how to handle attached e-mail files, scan them and, very important, report to the IT department any incident or situation that appears to be suspicious"

"Motivating and rewarding company employees with various bonuses or premiums to prevent them from leaving the company or disclosing important information to malicious outside people"

"Real and not formal communication between the staff responsible for organizational security and the rest of the employees"

"Raising employees' awareness of computer security, in order to prevent malware attacks"

together with "*a rigorous set of recruiting, selection, and hiring procedures"*, NDAs signing, *"adaptation of internal regulations to include rules on information security"*, and "*special training sessions for employees to prevent data loss"*.

Suggested ISPs revisions referred to *"no more BYOD"*, with a more focused advice, that *"employees who bring and use their own devices should be aware that a smart phone, tablet, laptop can be a big challenge for the company's IT department. It is important that every device that runs a different operating system has up-to-date security settings and is included in the company's secure network"*, and the monitoring of Internet activity for each employee.

In the communication area, students suggested *"a dedicated internal phone line and e-mail channel, to be used only inside the organisation when discussing confidential and secret information"*, and use of encryption.

Many references were made to backup procedures, as: *"investing in data backup and data recovery systems, as data in computing systems are vital to the firm", "more frequent backup, for not-so-important documents also", "a backup server/cloud solution"* or *"at least an UPS"*.

Other recommendations regarded "*written record of all services provided by the ICT Specialist, with date and signature on both sides, with all changes made to software and hardware*", *"contracting cloud services for the future online store of the shop, as developing a home-based solution involves colossal costs to ensure the security of the information stored on it, compared to storing the site on an online platform where security and maintenance is ensured in a professional way by the hosting provider"*, and "*testing the reaction times of the security firm that has never been done since signing the contract with them."*

5. Conclusions

The threats, vulnerabilities, adopted and needed security measures identified by the students during the study were very … earthly, unsophisticated and credible. Although the course largely presents sophisticated technical threats which are massively promoted in the media, such as Web Based Attacks, Web Application Attacks, Denial of Service, botnets, and adequate technical measures, these were ignored by analysts, as a result of their absence from the organizations under review. Their focus has been on the most common problems, frequently experienced in organisations, for which they have also selected the appropriate measures.

Beyond the modern and extremely interesting methods suggested by the literature, increasing the awareness of information security issues among SMEs' employees with a non-technical background can be done with modest means. The exercise we tried during the IS course had very good results: armed with minimal IS knowledge, the students analysed a familiar situation, in their immediate proximity, and presented the results using their own unsophisticated, natural language. The discussion which followed the analysis was in itself a good way to raise awareness at the level of our focus group. Good practices presented by each participant were saluted by the others, interesting questions arose, and some valuable lessons were learned during this workshop.

In conclusion, IS is rather a human problem than a technique one, and can be provided in a not very costly manner. Raising awareness amongst the employees and turning them into active

vectors, able to modify their own and their colleagues' behaviour regarding the IS are goals that can be achieved with a minimum investment in a basic IS course.

6. References

[1] ENISA, *ENISA Threat Landscape Report 2017*, January 2018. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017. [Accessed 1 February 2018].
[2] DC, *DDC Reveals Worldwide Internet of Things Predictions for 2015*, 3 December 2014. [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS25291514. [Accessed 2 October 2016].
[3] Royal Academy of Engineering, *Cyber safety. Strengthening the digital systems that support the modern economy*, Royal Academy of Engineering Prince Philip House, London, 2018.
[4] ENISA, *The new users' guide: How to raise information security awareness*, European Network and Information Security Agency (ENISA), 2010.
[5] Romanian National Computer Security Incident Response Team, *Awareness Guides*, 2018. [Online]. Available: https://cert.ro/. [Accessed 14 November 2018].
[6] Bitdefender, *Whitepapers*, 2018. [Online]. Available: https://www.bitdefender.com/. [Accessed 14 November 2018].
[7] L. A. Futcher, C. Schroder and R. von Solms, *An Integrative Approach to Information Security Education: A South African Perspective*, Information Management & Computer Security, 2010, vol. 18, no. 5, pp. 366-374,.
[8] B. Kooi and S. Hinduja, *Teaching Security Courses Experientially*, Journal of Criminal Justice Education, 2008, vol. 19, no. 2, pp. 290-307.
[9] T. Osburg and C. Lohrmann, Eds., *Sustainability in a Digital World: New Opportunities Through New Technologies*, Springer, 2017.
[10] A. Antonaci, R. Klemke, C. M. Stracke, M. Specht, M. Spatafora and K. Stefanova, *Gamification to Empower Information Security Education*, in GamiFIN Conference, Pori, Finland, 2017.
[11] B. Endicott-Popovsky, *Information Security and Risk Management*, coursera.org, 2014. [Online]. Available: https://www.coursera.org/course/inforiskman. [Accessed 8 January 2015].
[12] J. Van Niekerk and R. Goss, *Towards Information Security Education 3.0. A Call for Information Security Educational Ontologies*, in ISE 6, 7, and 8, IFIP AICT 406, IFIP International Federation for Information Processing, 2013, pp. 180-187.
[13] K. Salah, M. Hammoud and S. Zeadally, *Teaching Cybersecurity using the Cloud*, IEEE Transactions on Learning Technologies, vol. 8, no. X, 2015.
[14] Y. Alkhurayyif and G. R. S. Weir, *Evaluating Readability as a Factor in Information Security Policies*, in Proceedings of International Conference on Arts, Science & Technology, Dubai, 20-22 December 2017, 2017.