Available online at www.sciencedirect.com

ScienceDirect

Procedia - Social and Behavioral Sciences 147 (2014) 424 – 428

Procedia
Social and Behavioral Sciences

ICININFO

The Human Factor of Information Security: Unintentional Damage Perspective

Efthymia Metalidou[a,b], Catherine Marinagi[c], Panagiotis Trivellas[c], Niclas Eberhagen [b], Christos Skourlas[d]*, Georgios Giannakopoulos[a]

[a] Department of Librarianship and Information Systems, Department of Informatics, Technological Educational Institute of Athens, Ag. Spyridonos, GR12210, Athens, GREECE
[b] Department of Informatics, Linnaeus University, SE-35139, Växjö, SWEDEN
[c] Department of Logistics, Technological Educational Institute of Central Greece, GR32200, Thiva, GREECE
[d] Department of Informatics, Technological Educational Institute of Athens, Ag. Spyridonos, GR12210, Athens, GREECE

Abstract

It is widely acknowledged that employees of an organization are often a weak link in the protection of its information assets. Information security has not been given enough attention in the literature in terms of the human factor effect; researchers have called for more examination in this area. Human factors play a significant role in computer security. In this paper, we focus on the relationship of the human factor on information security presenting the human weaknesses that may lead to unintentional harm to the organization and discuss how information security awareness can be a major tool in overcoming these weaknesses. A framework for a field research is also presented in order to identify the human factors and the major attacks that threat computer security.

Selection and peer-review under responsibility of the 3rd International Conference on Integrated Information.
Keywords: information security; information security awareness; human factors; reliability

* Corresponding author. Tel.: +30-2105910974; fax: +30-2105910975
E-mail address: cskourlas@teiath.gr

Selection and peer-review under responsibility of the 3rd International Conference on Integrated Information.
doi:10.1016/j.sbspro.2014.07.133

1. Introduction

Human factor has a tremendous impact on the success and failure of our efforts to secure and protect our businesses, services, systems, and information (Orshesky, 2003). According to Kearney (2010), if security loopholes are missed by the process designer, the strength of the IT system becomes a weakness that can be exploited by an attacker – a weakness that can be exploited repeatedly in just a small amount of time. A major concern within information security is the threat of social engineering attacks. Attackers, using social engineering, attempt to gain sensitive information, targeting human vulnerabilities – that is, weaknesses in an organization's security due to the characteristics and behaviors of people. The European Security Forum (1993) defines information security awareness as "the degree or extent to which every member of staff understands: 1) the importance of information security 2) the levels of information security appropriate to the organization 3) their individual security responsibilities, and acts accordingly. Information security refers to the protection of the confidentiality, integrity and access [availability] to information (Kruger & Kearney, 2006).

The purpose of this paper is to review the human factor in information security and discuss how information security awareness can be a major tool in overcoming these weaknesses. The rest of the paper is organized as follows: Section 2 presents literature review. Section 3 presents a framework to examine the correlation of Human Factors with the Lack of Information Security Awareness. Section 4 discusses how to raise awareness, in order to overcome weaknesses. Finally, Section 5 concludes the paper.

2. Literature Review

The increased threats of information technology brought new solutions focused on technological means, while the human factor related research has been limited; with the only notable exception of password generation (Ahmed & Siyal, 2005; Sheng et al., 2012). Many times organizations overlook the human factor, a factor that security depends upon (Kahraman, 2005). Technology is often falsely perceived as the immediate answer to Information Security problems (Hinson, 2003). Information Security is primarily a human factors problem that remains unaddressed (Schultz, 2005). A security survey from Cisco Systems revealed that users who work remotely, although they claim to have awareness of security risks, would still engage into actions which endanger the system security (Panko, 2004). When a user has poor training, even an ideal and flawless software or hardware solution will still not be of any use (Sapronov, 2005). In spite of the latest technological improvements in security, it is still the network users who are often unknowingly inviting security breaches through carelessness and a lack of awareness (Danchev, 2006). According to Deloitte (2009), human error is overwhelmingly stated as the greatest security weakness in 2009 (86%), followed by technology (a distant 63%).

A serious vulnerability is social engineering, which is a highly effective attack, which bypasses every technological protection (Schneier, 2000). A study examining the behavior of employees showed that upon receiving email that was designed to look suspicious, 37% would not only open the email, but would actually click on the link provided; while 13% would open the attached file. Additionally, upon receiving an email that was designed to appear legitimate, 42% followed a web link and provided sensitive information, while 30% run an attached executable file, which would supposedly improve computer performance (Kruger, Drevin & Steyn, 2007). Panko (2004) suggests that for designing or auditing security operations, the principle of having clear roles should be implemented, i.e. the roles define who does what and determine procedures.

3. Towards a framework for Information Security Awareness and Human Factors

In this section, we want to establish a framework to examine the correlation of Human Factors with the Lack of Information Security Awareness.

Kraemer et al. (2009) describe how human and organizational factors may be related to technical computer and information security (CIS) vulnerabilities. According to Kraemer et al. (Kreamer et al., 2009) we "should be aware of the multifarious roles of human and organizational factors and CIS vulnerabilities and that CIS vulnerabilities are not the sole result of a technological problem or programming mistake."

Badie and Lashkari (2012) propose the categorization of the factors, which affect security of computers, into two main categories namely human factor and organization factor and they believe that the review of previous research work shows that human factor is most important than the other factors. They also propose the division of the human factors into two groups: 1) factors that belong to management, namely workload and inadequate

staffing, and 2) factors related to end user, namely, lack of awareness, (risky) belief, (risky) behavior, inadequate use of technology, lack of motivation. Their choice of these factors is based on the research of Kraemer et al. (2009), which categorized the human factors into nine (9) areas: external influences, human error, management, organization, performance and resource management, policy issues, technology, and training. In the following, we focus on the five human factors determined by Badie and Lashkari (2012) that have serious implications to end users' behavior.

Lack of Motivation

Parsons et al. (2010) believe that "Employees need to be motivated to adopt secure behaviours and practices, and management need to be able to identify what motivates their staff". According to Koh et al. (2005) motivation occurs when security issues are shared and users are involved in decision making in order to follow security procedures.

Lack of awareness

Lack of awareness is related with a lack of general knowledge about Attacks. Common examples of lack of awareness could be the following: Users do not know how to see a sign of a spyware on their computer, and how important is to specify a strong password, they cannot protect themselves from identity theft, and social engineering, and they do not know how to control the access of others to their computer. Albrechtsen (2007) claim that "general awareness campaigns have little effect alone on user awareness".

Belief

The term belief could be interpreted as the Users' Risky Belief for CIS. Albrechtsen (2007) conducted a qualitative study of users' view on information security and presented various erroneous beliefs. For instance, Albrechtsen underlined that users usually "felt their behaviour was in compliance with the documented system due to the belief that the rules and guidelines are common sense". Common examples of risky belief are the following: Users believe that the installation of anti-virus software is not crucial for their information, or they are ready to click on a link while they receive an email from unknown persons.

Behavior

The term behavior could be interpreted as the users' risky behavior or the loss of prevention behavior. Such a behavior could be created by several factors. Albrechtsen (2007) claims that "Documented requirements of expected information security behavior have little effect alone on user behavior". It is worth of mentioning the following conclusion of Albrechtsen: "The users consider a user-involving approach to be much more effective for influencing user awareness and behavior".

Inadequate Use of Technology

Even the finest technology cannot succeed in solving information security problems without the continuous human cooperation and the effective use of this technology. Common examples of inappropriate uses of technology are the following: making unauthorized reconfiguration of systems, accessing passwords of others, retrieving inappropriate information. Ngo (2008) believes that "giving individuals knowledge of IT security basics such as threats, risks, and consequences of their actions will allow individuals to gradually adapt to constant change and hence allow us to predict expected behavior".

Computer security risks

Information security breaches can be categorised in a number of different ways. Badie and Lashkari (2012) based on several studies performed by other researchers presented 13 attacks which cover all of the computer security risk factors, and eventually defined "9 factors (that) can cover all risks as main factors". These factors are: Excess Privilege, Error and Omission, Denial of Service, Social Engineering, Unauthorized Access, Identity Thief, Phishing, Malware, and Unauthorized Copy.

4. Raising security awareness

As we can see from the previous sections, raising security awareness is the key to limiting the number of breaches caused by human weaknesses (Mitnik & Simon, 2002; Kearney, 2010; Thomson & Van Niekerk, 2012). The way to raise awareness, resulting in overcoming the aforementioned weaknesses, is presented in this section. Before we can expect people or systems to protect our information and our infrastructures, we should know what we have, what is worth, and what is at risk. Most organizations have quite valuable information and services in the control of people who are not aware of its value, the importance of maintaining its protection, or the implications if that information is exposed (Orshesky, 2003). According to Kearney (2010), people can only help in preventing security breaches, if they are aware of the dangers, and are taught secure behaviors as part of their normal work training. However, a common hindrance to the creation of an environment where management and employees are working towards the same information security goals is the apathy of employees (Thomson & Van Niekerk, 2012). Every organization must promote a culture in which employees share the responsibility of defending the company against attack (Kearney, 2010). To ensure that a policy is implemented and effective, the policy must first be understandable. Not understanding what is expected of them, employees find it difficult to comply. Policy that does not take into account the objectives of the business, and fails to recognize the business mission, is sure to be overlooked every time it interferes with productivity or generating revenue (Orshesky, 2003). We have also to take into account that when employees feel committed to their job, they are more likely to feel satisfied with the job and be motivated to perform at their best. A survey reported in (Trivellas, 2011) confirmed the mediating role of employees' organizational commitment to work motivation and job performance. Offering training is one of the factors that increase employees' level of satisfaction. However, employees' training on security risks and measures against attacks should be carefully organized. Thomson and Niekerk (2012) indicate that instructions or orders will only influence behavior if they are consciously accepted by each employee and then translated into specific goals. When a person perceives that the achievement of a goal is not possible, commitment diminishes considerably (Layton, 2005). Therefore, it must be ensured that information security goals are perceived as attainable to ensure commitment. Policies have to be readily accessible or available to employees to ensure that they will not be ignored. It should be clear to all employees what their exact role and responsibilities are concerning security.

5. Conclusion

Users want both security and flexibility, and finding a balance between these two factors is a challenging task each organization has to face. There is a constant battle between attackers and security professionals, where users have the ability to swing the balance one way or the other: unfortunately, the unpredictability (or predictability) of human behavior can turn the most secure Information Systems into nothing.

An attempt was made in this study, to gather and clearly identify the human weaknesses causing security issues and provide suggestions on ways to overcome them. The implication of this study is that information security awareness is the key to mitigate security threats caused by human weaknesses. Organizations need to cultivate and maintain a culture where positive security behaviors are valued; they need to instill in their culture that security begins and ends with each person involved with their infrastructures, their businesses, and their services. The challenges associated with information security that employees face on a daily basis need to be understood and resolved. This means that security functions have to be meaningful and as little intrusive as possible. In addition, security policies need to be comprehensible and easy to locate. Employees' education about the importance of security awareness should be a priority of the organization.

For when the computers and technology fail, it is ultimately the people who depend on the services provided by that infrastructure that suffer (Orshesky, 2003).

References

Albrechtsen E. (2007). A qualitative study of users' view on information security, Computers & Security, vol. 26, 276-289

Ahmed, F., & Siyal, M.Y. (2005). A novel approach for regenerating a private key using password, fingerprint and smart card. *Information Management & Computer Security*, 13, 1, 39-54.

Badie, N., & Lashkari, A. H. (2012). A new Evaluation Criteria for Effective Security Awareness in Computer Risk Management based on AHP. *Journal of Basic and Applied Scientific Research*, 2, 9, 9331-9347.

Danchev, D. (2006). Reducing "Human Factor" Mistakes. Available: http://www.windowsecurity.com/articles/Reducing_Human_Factor_Mistakes.html [accessed: 03 July 2012].

Deloitte (2009). Protecting what matters. 6th Annual Global Security Survey.

European Security Forum (1993). Implementation Guide: How to make your organization aware of IT Security. *European Security Forum*, London.

Hinson, G. (2003). Human factors in information security. IsecT Ltd. Available: http://www.noticebored.com/NB_White_paper_on_human_factors_v5.pdf [accessed: 02 August 2012].

Kahraman, E. (2005). *Evaluating IT security performance with quantifiable metrics*. Master's thesis, DSV SU/KTH.

Kearney, P. (2010). *Security: The Human Factor*. Cambridgeshire: IT Governance Publishing.

Koh, K., Ruighaver, A.B, Maynard, S. & Ahmad, A. (2005). Security governance: its impact on security culture. Proceedings of the Third Australian Information Security Management Conference, Perth, Australia, September.

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security,* 28, 7, 509-520.

Kruger, H., & Kearney, W.D. (2006). A prototype for assessing information security awareness. *Computers and Security*. 25, 289-296.

Kruger, H., Drevin, L., & Steyn, T. (2007). *Email Security Awareness: A Practical Assessment of Employee Behaviour*. North-West University.

Layton, T.P. (2005). *Information Security Awareness – The Psychology behind the Technology*. Bloomington IN: AuthorHouse.

Mitnik, K., & Simon, W. (2002). *The Art of Deception*. Wiley Publishing Inc..

Ngo, L., (2008), IT Security Culture Transition Process, IGI Global encyclopedia, Encyclopedia of Information Ethics and Security, 319-325

Orshesky, C. (2003). Beyond technology - The human factor in business systems. *Journal of Business Strategy*, 24, 4, 43-47.

Panko, R. (2004). *Corporate Computer and Network Security*. Pearson Education Inc..

Parsons, K., McCormac, A., Butavicius, M. & Ferguson, L. (2010). Human Factors and Information Security: Individual, Culture and Security Environment. Command, Control, Communications and Intelligence Division DSTO Defence Science and Technology Organisation, Edinburgh South Australia

Sapronov, K., (2005). The human factor and information security. Available: http://www.securelist.com/en/analysis?pubid=176195190 [accessed: 12 July 2012].

Schneier, B. (2000). *Secrets and Lies*, New York: John Wiley & Sons.

Schultz, E. (2005). The human factor in security. *Computers & Security*, 24, 425-426.

Sheng, W., Howells, G., Fairhurst, M., Deravi, F., & Chen, S. (2012). Reliable and secure encryption key generation from fingerprints. *Information Management & Computer Security*, 20, 3, 207 – 221.

Trivellas, P. (2011). Work motivation and job performance of frontline employees: the mediating role of organizational commitment, International Conference on Industrial Engineering and Engineering Management (IEEM 2011), Dec 6-9, Singapore, 1878-1882

Thomson, K., & Van Niekerk, J. (2012). Combating information security apathy by encouraging prosocial organisational behavior. *Information Management & Computer Security*, 20, 1, 39-46.