JPM
JOURNAL OF POSITIVE MANAGEMENT
Vol. 8, No. 1, 2017, pp. 78–85

ISSN 2083-103X

http://dx.doi.org/
10.12775/JPM.2017.006

FORMING THE AWARENESS OF EMPLOYEES IN THE FIELD OF INFORMATION SECURITY

Joanna Chmura

Nicolaus Copernicus University in Toruń,
Faculty of Economic Sciences and Management, Toruń, Poland

e-mail: jchmura@doktorant.umk.pl

Abstract

Research purpose: The aim of this study is to present the essence and importance of information security awareness in the organisation and to analyse selected methods used in forming employee awareness in terms of information security.

Methodology/ approach: This paper is based on literature studies and available reports.

Findings: The presented paper suggests that in order to create a positive change in the organisation, information security training should focus on the attitude and behavior of employees. Concentration is primarily about what they do and how their actions affect the results. In order to minimise the risk of data breaches, often resulting from human error, training methods must meet the needs of today's employees. Effective information security awareness strategies should address the needs of both the organisation itself and the learning people.

Limitations/implications: The study is based on the theoretical analysis, indicating the need of conducting further empirical research.

Originality/value: The main value of the study is to clarify the need for forming employees' awareness of information security, while indicating a number of available methods enabling the implementation of awareness programs in the organisation.

Keywords: information security, information security awareness, method, training

Paper type: Conceptual paper

1. Introduction

The dynamic development of information technologies which happened in recent years, has made information security issues a major concern of today's organisations. *Global Information Security Survey* conducted by EY (2017) shows that despite the implementation of state-of-the-art inspection techniques, enterprises continue to experience numerous security breaches. The research results show that the greatest security vulnerability is the lack of the awareness of employees (2013 – 53%, 2014 – 57%, 2015 – 44%, 2016 – 55%) (EY, 2017).

In addition, the analysis of the cited studies highlights that security incidents in organisations, predominated the number of events recorded outside.

Based on the above reports, it can be assumed that the human factor plays a key role in the implementation of the information security system. Many authors rightly point out that technical means alone are no longer sufficient to ensure information security in an organization (Vroom and Solms, 2004; Schultz, 2005; Kritzinger and Smith, 2009; McCormac et al., 2017). Mitnick and Simon point out that people are the weakest link in the information security chain (Mitnick and Simon, 2002). Therefore, in the face of modern threats, particular attention should be paid to the human dimension (Thomas et al., 2006; Kraemer et al., 2009). One way to help this process is to build employee awareness in information security.

The subject of the article regards the analysis of the available methods used to educate employees about information security. This article is a review based on literature studies, which is the basis for further empirical research. The work was divided into 5 parts. Part 1 is an introduction to the topic of information security, pointing the problem of the employees' lack of awareness regarding information security based on the EY 2016 study. Part 2 provides a review of literature describing assumptions about information security awareness. Part 3 presents a list of selected methods used to raise awareness of information security. A discussion of ongoing considerations is provided in part 4. In turn, part 5, summarises the work, pointing to the direction of further research.

2. Literature review

Most of the information security studies is focused on purely technical aspects. However, as the interest in the issue increases, the number of research studies on the importance and measurement of individuals' awareness and behavior regarding information security increases.

Researchers determine in various ways the issue of employee awareness of information security (Öğütçü et al., 2016). According to Kruger and Kearney, information security is perceived as the degree to which every employee understands the importance and consequences of security policies, internal guidelines for information security organizations (Kruger and Kearney, 2006). The cited definition of information security awareness refers fully to the KAB model that forms the basis of the HAIS-Q research instrument (Parsons et al., 2014; 2017). The mentioned method of measuring consciousness relies heavily on techniques borrowed from social psychology, which suggests that the tendency of a person to do something beneficial or unfavorable depends on three components, namely knowledge, attitude and behavior. The KAB model essentially explains the role of knowledge in behavior change. The cumulation of these three factors shows that knowledge leads to a change of attitude, and this in turn changes behavior. Khan et al. (2011) confirm the influence of knowledge on the behavior of

people, which in turn leads to changes in attitudes and behavior in consciousness. Similarly, Aurigemma and Panko (2012) point out that the overall success of information security depends on the effective user behavior.

It is assumed that the increased employee awareness of information security should minimise the risk of employee behavior, focusing mainly on the set of learning experiences. Parsons et al. (2014) indicate that awareness and training are the two most effective mitigating measures for human activities. In addition, COBIT [1] emphasizes the importance of building awareness in information security at both individual and organisational levels. Similarly, the Organisation for Economic Co-operation and Development (OECD) [2] points out, emphasizing the need to develop a strong culture of information security through various factors, including training and awareness.

Learning is one of the basic elements for creating information security awareness. According to the attitude ofSchlienger and Teufel, training programs on safety awareness can be divided into three different sections, i.e.(Schlienger and Teufel, 2003):

- Education,
- Training,
- Awareness.

The interpretation of these three factors demonstrates that employees need to understand why information security is so important to the organisation and that each employee is responsible for safety in his or her field of work. The element of education can be realised through specialised information security courses conducted at universities.

In case of training, employees need to know how they can feel secure and how to use security features in their applications in the process of work. In this case, it is recommended to conduct the training on special tools and security features of the applications. Both education and training form the basis of the safety program, but do not guarantee full compliance of safety behavior in everyday work life. Therefore, the measurement of consciousness outside the training room reminds workers to draw conclusions. In addition, the incentive programmes significantly encourage participation all over the system, while changing the security culture in the organisation.

As regards the above considerations, it is theoretically assumed that increasing information security awareness is an important part of the holistic approach to managing information security (Samroo et al., 2016). Building safety awareness is primarily aimed at increasing the users' understanding of how to follow proper practices and why it is necessary (Maqousi et al., 2013, Tsohou et al., 2015). Shaw et al. (2009) emphasize that information security awareness is as important as ensuring that information is relevant and consistent (Shaw et al., 2009).

3. The analysis of methods in the field of forming security awareness

Both on theoretical and practical ground, there are many methods used to build information security awareness, each of which has both advantages and disadvantages. A wide variety of information security knowledge delivery methods often provide organisations with many difficulties (Valenine, 2006).
In order to conduct a detailed analysis of available methods, the following division of methods was adopted in the study:

- traditional methods,
- methods based on eduactional games and films,
- the Internet methods.

3.1. Traditional methods

Traditional methods used in forming information security awareness include both paper and electronic resources. Information leaflets, posters, newsletters, and educational presentations, which provide information on password, email, anti-virus protection management, as well as general rules regarding information security in organisations, are often used in information campaigns on security information (Abawajy, 2014).

Posters are commonly used to announce a particular information security issue. They are shared in designated locations to give more attention to employees, reminding them of the specific actions that need to be taken to improve security in the organisation. They also serve to periodically strengthen information security. The main concern with using this type of tool is the fact of omission of messages that have been placed on the poster.

Newsletters, in turn, aim to strengthen information security programmes. They can be both paper and electronic.They include the ability to send multiple messages at the same time as opposed to the posters. Concerns arise in this case mainly due to the fact that there is no guarantee that employees are familiar with the content of the newsletter and understand the content contained therein.

The advantage of traditional methods is primarily the low cost of implementing information campaigns. However, as Khan et al. (2011) provide, the lack of social norms that are more effective in causing intentions, makes these methods less effective.

3.2. Methods based on educational games and films

The alternative way of providing knowledge in information security are methods based on educational games and film**.**

Games that stimulate information security knowledge combine both fun and training. Such methods are highly interactive, so they are used to support security objectives in the organisation, while involving the user. Games are a good technique for motivating a player to adapt the behavior to information security.

The interactive character of the game has a significant impact on the change attitude of the user, but it is not the best source for providing detailed information about information security policy (Cone et al., 2006).

Educational films play an important role in the awareness programmes. The formula of this method provides participants with the opportunity to study their own knowledge at any time, without any time constraints. Learners can start and finish training at any time. The interactivity of this method makes educational films more effective than traditional methods of providing security knowledge. The limitation of introducing this way of forming awareness is the cost of its implementation and the lack of interaction between the trainer and the training participant.

3.3. The Internet methods

The Internet methods used in awareness campaigns include e-mail, blogs, animations and multimedia. The methods made available on the Internet, despite some limitations, are considered to be most effective in providing information related to safety (Abawajy, 2014). One of the most frequently used Internet method are e-mail messages, which are employed in the organisations, in order to form the awareness. They serve mainly to provide information and knowledge, highlighting important security issues. They remind the users about specific actions that are to be conducted, in order to improve the attitude towards security in the organisation. The effectiveness of this method is limited by the lack of guarantee that the messages will be read and the content understood.

4. Discussion

The human factor often determines success or failure in managing information security. Each security breach incident in an organisation is more or less dependent not only on technology but primarily on the end users (Hadlington, 2017). In order to mitigate the risk of information security, the organisations are required to implement an appropriate awareness program for all employees.

The aim of this study was to present the essence and importance of information security awareness as well as to analyse selected methods used in forming the employee awareness in information security. This analysis shows that, despite some limitations, the increasing employee awareness of information security is largely dependent on the method of providing knowledge. In addition, literature studies have confirmed that awareness-raising methods and techniques, such as trainings and communication, are effective in enhancing user safety knowledge, including promotion of appropriate attitudes and behavior. Only aware employees are able to prevent events related to the loss of information resources in the organisation. To achieve this, information security awareness programs should be provided through appropriate methods adapted to the culture of the organisation.

In addition, Eminağaoğlu et al. (2009) emphasize in their research that, in addition to standard training, organisations should periodically introduce awareness campaigns supplemented by additional interactive support materials.

5. Conclusions and future research

The EY (2017) Information Security study indicates that raising employee awareness is one of the key challenges faced by organisations around the world. Information security awareness programmes are a key element of today's organisation's strategy. The long-term goal of implementing such a program is first and foremost to achieve lasting change in employee attitudes by promoting a safety culture and developing appropriate habits. To meet new challenges that are relevant to today's threats, it is imperative to implement a comprehensive approach to information security in the organisation. This is also highlighted by the European Network and Information Security Agency (ENISA), which indicates that awareness of dangers and risks should be the first line of defence for information security. Systematic awareness-raising campaigns for information security users can greatly influence the change in information security attitudes in organisations.

Information security awareness is a dynamic process, dependent on ever-changing threats. It is therefore considered that any safety awareness program should be subject to continuous monitoring, thus forming an integral part of the company's culture. Stimulating effective training and awareness of information security at all levels of the organisation can contribute to the promotion of a positive security culture, thereby increasing the protection of information (Da Veiga, 2015).

Notes

[1] Control Objectives for Information and related Technology.
[2] Organisation for Economic Co-operation and Development.

References

Abawajy, J. (2014), „User preference of cyber security awareness delivery methods", *Behaviour & Information Technology,* Vol. 33 No. 3, pp. 236–247. DOI: 10.1080/0144929X.2012.708787

Aurigemma, S., Panko, R. P. (2012), „A Composite Framework for Behavioral Compliance with Information Security Police", *47th Hawaii International Conference on System Sciences,* pp. 3248–3257. DOI: 10.1109/HICSS.2012.49.

Cone, B. D., Thompson, M. F., Irvine, C. E., Nguyen, T. D. (2006), „Cyber Security Training and Awareness Through Game Play", in: Fisher-Hubner, S., Rannenberg, K., Yngstrom, L., Lindskog, S. (Eds.), *Security and Privacy in Dynamic Environments,* International Federation for Information Processing, Vol. 201, Boston: Springer, Boston, pp. 431–436.

Da Veiga, A. (2015), „An Information Security Training and Awareness Approach (ISTAAP) to Instil an Information Security – Positive Culture", *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015),* pp. 95–107.

Eminağaoğlu, M., Uçar, E., Eren, S. (2009), „The positive outcomes of information security awareness training in companies – A case study", *Information Security Technical Report,* Vol. 14 No. 4, pp. 223–229.

EY (2017), „Path to cyber resilience: EY's 19th Global Information Security Survey 2016-2017", available at: http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2016-pdf/$FILE/GISS_2016_Report_Final.pdf (accessed 3 September 2017).

Hadlington, L. (2017), „Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours", *Heliyon,* Vol. 3 No. 7, pp. 1–18. DOI: 10.1016/j.heliyon.2017e00346

Herold, R. (2010), *Managing an Information Security and Privacy Awareness and Training Program, Second Edition,* CRC Press, Inc. Boca Raton, FL, USA.

Kajzer, M., D'Arcy, J., Crowell, Ch.R., Striegel, A., Bruggen, D.V. (2014), „An exploratory investigation of message-person congruence in information security awareness campaigns", *Computers & Security,* Vol. 43, pp. 64–76. DOI: 10.1016/j.cose.2014.03.003

Khan, B., Alghathbar, K.S., Nabi, S.I., Khan, M.K. (2011), „Effectiveness of information security awareness methods based on psychological theories", *African Journal of Business Management,* Vol. 5 No. 26, pp. 10862–10868. DOI: 10.5897/AJBM11.067

Ki-Aries, D., Faily, S. (2017), „Persona-centred information security awareness", *Computers & Security*, Vol. 70, pp. 663–674. DOI: 10.1016/j.cose.2017.08.001

Kraemer, S., Carayon, P., Clem, J. (2009), „Human and organizational factors in computer and information security: Pathways to vulnerabilities", *Computers & Security*, Vol. 28 No. 7, pp. 509–520. DOI: 10.1016/j.cose.2009.04.006

Kritzinger, E., Smith, E. (2009), „A prototype for enhancing information security awareness in industry", *Proceedings of the World Academy of Science Engineering and Technology,* Vol. 54, pp. 521–530.

Kruger, H.A., Kearney, W.D. (2006), „A prototype for assessing information security awareness", *Computers & Security,* Vol. 25 No. 4, pp. 289–296. DOI: 10.1016/j.cose.2006.02.008

Maqousi, A., Balikhina, T., Mackay, M. (2013), „An effective method for information security awareness raising initiatives", *International Journal of Computer Science & Information Technology*, Vol. 5 No. 2, pp. 63–72. DOI: 10.5121/ijcsit.2013.5206

Mitnick, K.D., Simon, W.L. (2002), *The Art of Deception: Controlling the Human Element of Security,* Wiley, New Jersey.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., Pattinson, M. (2017), „Individual differences and Information Security Awareness", *Computers in Human Behavior,* Vol. 69, pp. 151–156. DOI: 10.1016/j.chb.2016.11.065

Mukhlis, A. (2014), „Information security awareness level measurement using multiple criteria decision analysis (MCDA)", *Jurnal Penelitian dan Pengembangan Komunikasi dan Informatika,* Vol. 5 No. 1, pp. 15–24.

Öğütçü, G., Testik, Ö.M., Chouseinoglou, O. (2016), „Analysis of personal information

security behavior and awareness", *Computers & Security*, Vol. 56, pp. 83–93. DOI: 10.1016/j.cose.2015.10.002

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., Jerram, C. (2014), „Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)", *Computers & Security*, Vol. 42, pp. 165–176. DOI: 10.1016/j.cose.2013.12.003

Parsons, K., Calic, D., Pattinsonb, M., Butaviciusa, M., McCormaca, A., Zwaansc, T. (2017), „The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studie", *Computers & Security*, Vol. 66, pp. 40–51. DOI: 10.1016/j.cose.2017.01.004

Schlienger, T., Teufel, S. (2003), „Information Security Culture – from analysis to change", *South African Computer Journal,* Vol. 2003 No. 31, pp. 46–52.

Schultz, E. (2005), „The human factor in securiy", *Computers & Security*, Vol. 24 No. 6, pp. 425–426.

Shaw, R.S., Charlie, Ch.C., Harris, A.L., Huang, H-J. (2009), „The impact of information richness on information security awareness training effectiveness", *Computers & Education,* Vol. 52, pp. 92–100. DOI: 10.1016/j.compedu.2008.06.011

Soomro, Z.A., Shah, M.H., Ahmed, J. (2016), „Information security management needs more holistic approach: A literature review", *International Journal of Information Management,* Vol. 36 No. 2, pp. 215–225. DOI: 10.1016/j.ijinfomgt.2015.11.009

Thomson, K., von Solms, R., Louw, L. (2006), „Cultivating an organisational information security culture", *Computer Fraud and Security,* Vol. 2006 No. 10, pp. 7–11.

Tsohou, A., Karyda, M., Kokolakis, S. (2015), „Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs", *Computers & Security,* Vol. 52, pp. 128–141. DOI: 10.1016/j.cose.2015.04.006

Valentine, J.A. (2006), „Enhancing the employee security awareness model", *Computer Fraud & Security,* Vol. 6, pp. 17–19.

Vroom, C., Von Solms, R. (2004), "Towards information security behavioural compliance", *Computers & Security,* Vol. 23 No. 3, pp. 191–198.