BUILDING AN EFFECTIVE INFORMATION SECURITY AWARENESS PROGRAM

Ildikó Legárd[1]

DOI: 10.24989/ocg. 338.15

Abstract
Many researchers and experts in the field of information security agree that the user is the weakest link in an organization's chain of information security. Even if the system's and the stored data's physical and logical protection is well developed, the human factor exposes security to significant risk. The effective protection against the threats is to provide security awareness through implementing a well-developed and successful Information Security Awareness Program.

Although organizations are able to recognize the importance of information security awareness, the implementation of the awareness programs can be difficult. The aim of this study is to help organizations to develop an effective Information Security Awareness Program tailored to the characteristics of the organization. The paper presents how we can build a program that influences and improves the user's knowledge, attitude and behavior the most towards information security and makes positive changes in the security culture of an organization. To achieve that goal, the study identifies the key elements of the implementation, compares traditional awareness programs with modern trainings and highlights the importance of communication channels and methods. There is no single solution to improve information security, the essay summarizes and shows the most effective techniques that experts can use in order to seize the user's attention toward information security, to establish credibility and trust, and to motivate action.

1. Introduction

Technological advances in recent decades, the rapid increase in digitalization, the tremendous development of ICT tools and services, the widespread use of the Internet, and rapid access have irreversibly changed the lives of people, the way businesses operate and the organization of public administration. In parallel with the incessant development, the fight for obtaining data and information stored in information systems and for influencing the operation of the systems also started to become sophisticated, while the security awareness of the users of these systems did not keep track with the pace of technical development. Not surprisingly, cyber criminals have begun using a new and very popular form of attack, called social engineering that builds on influencing, manipulating and exploiting the vulnerability of the human factor.

„Social engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation."- said Kevin Mitnich, once known as "The World's Most Wanted Hacker".[2] According to Mitnich, as a result, the social engineer can use people to gain information with or without technology.

[1] Doctoral School of Public Administration Sciences, National University of Public Service, H-1083 Budapest, Üllői út 82., ildiko.legard@gmail.com, www.uni-nke.hu
[2] Kevin Mitnick, "The World's Most Famous Hacker," was born in Los Angeles, CA in 1963. In the late '80s and early '90s, Mitnick used social engineering to hack the computer systems of various companies.

Broadhurst and Chantler argued, that the employees become the primary target for social engineers and cyber criminals, as the first step is gaining access to information. „The secondary target, such as the organisation's computer system; which in turn may lead to a tertiary or main target such as a system control program, database, financial or telecommunication system. Cyber criminals will try to gain this 'access information' enabling them to bypass security. This can include usernames and passwords, PIN's (personal identification numbers), tokens and credit card information (Federal Communications Commission 2002). Once they have gained access to the system, they are then able to erase, modify or copy the information to suit the needs of their attack." [1, p. 1]

Social engineering attacks can be divided into two groups, depending on the methods used by the attacker: human-based and computer-based forms of attack. The most popular forms of the human-based attacks are: asking for aid or support, assistance (reverse social engineering), identity theft, thumbstone theft, shoulder surfing, dumpster diving and tailgating. The computer-based attacks are: phishing (for example scam, vishing, smishing, pharming, whailing), malicious programs (for example: viruses, trojans, scripts, keylogger, spyware, baiting, ransomware), attacks based on public Wi-Fi and attacks based on mobile apps. [2] [3] [4]

Effective protection against these threats can be ensured by the security awareness of the users, which can be achieved through a well-organized and successful security awareness program.

This paper is structured as follows. After an introduction, section 2 presents the methodology of this research. Section 3 reviews the conceptual framework including information security, information security awareness and information security awareness programs. Section 4 examines the main factors influencing the effectiveness of information security awareness programs, identifies the key elements of the programs' planning and implementation and summarize the most important components of a successful awareness program involving training material, methods, communication channels and scheduling. Finally, section 5 draws the main conclusions of the study.

2. Methodology

This study utilizes the qualitative method of research for an analysis of the factors and potential pitfalls for security awareness programs' success and introduces a set of tools that can help organizations choosing appropriate communication channels and methods to transfer basic knowledge of information security to the users. The qualitative research in this study is based on a secondary analysis of literature. That type of analysis reviews traditional as well as recent developments in the field of security awareness programs and allows an „in-depth analysis of findings of original primary studies" [5, p. 2].

The study used Scopus, ScienceDirect and Google Scholar databases in order to find literature that presents the key elements of effective information security awareness programs and identify the challenges of their implementation. The research utilized the use of keyword patterns – "information", "security", "awareness", "program"-, in order to search for relevant literature or articles. I searched

According to his Wikipedia page, in 1999, Mitnick pleaded guilty to four counts of wire fraud, two counts of computer fraud and one count of illegally intercepting wire communication. He would go on to serve five years in prison followed by three years of supervised release during which time he was forbidden to use a computer.
Today Mitnick runs Mitnick Security Consulting LLC, a computer security consultancy and is part owner of KnowBe4, a provider of security awareness training, that also provides anti-phishing software like PhishProtection.com. He does computer security consulting and penetration testing for Fortune 500 companies as well as the FBI. https://www.phishprotection.com/heroes/kevin-mitnick/ [Accessed: January 14, 2020].

literature published between 2015-2019, and I got 279 relevant paper with these keywords based on Scopus. In order to filter out the most relevant studies I firstly identified the most cited authors (Aldawood, H.; Skinner, G.; Calic, D; Da Veiga, A.; McCormac, A.; Parsons, K; Pattinson, M.; Tsohou, A.), universities (University of South Africa, The University of Adelaide, North-West University, Korea University, Goethe Universität Frankfurt), and countries (United States, South Africa, United Kingdom, Australia, Germany). I reviewed the most cited authors' studies used ScienceDirect and Google Scholar and then from their references I could select the other important documents for my study.

3. Conceptual framework

3.1. Information Security

According to Kruger and Kearney „whilst information security generally focuses on protecting the confidentiality, integrity and availability of information, information security awareness deals with the use of security awareness programs to create and maintain security-positive behavior as a critical element in an effective information security environment". [6]

NATO's interpretation of Information Security (INFOSEC) by Allied Joint Doctrine For Information Operations: As part of OPSEC (Operations Security) the goal of Information Security (INFOSEC) is to protect information (stored, processed or transmitted), as well as the host systems, against a loss of confidentiality, integrity and availability through a variety of procedural, technical and administrative controls. INFOSEC includes a range of measures that are applied on a routine basis under the auspices of security policy to protect information. INFOSEC is an integral element of all military operations and encompasses Communications Security (COMSEC), Computer Security (COMPUSEC), Computer Network Defense (CND), an integral part of Computer Network Operations (CNO), and together with personnel, document, physical and procedural security, it must be considered at the earliest conceptual stages and throughout the planning of an operation. [7]

Information Security plays an important role in preventing and mitigating the impact of different security threats like social engineering attacks. There are various types of measures under Information Security (for example modern preventive tools and security systems in place) and one of them is Information Security Awareness. [8, p. 62.]

3.2. Information security awareness

Although security literature emphasizes the importance of developing security awareness and security awareness programs, but surprisingly, the commonly accepted definitions for security awareness and security awareness program are missing.

Shaw et al. [9] in the article "The impact of information richness on information security awareness training effectiveness" use the following definition: "Security awareness is the degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information security control to protect the organization's data and networks". [9, p. 63.] Aldawood and Skinner highlight the users' ability to recognize, flag, evade and disable malicious attempts of an attack. [5, p. 2]

Nemeslaki and Sasvári [10] emphasize the organizational aspects of the definition, such as information security awareness is part of an organization's culture, a way of thinking and behaving

that ensures that employees within organizations are aware of and are ideally committed to the security objectives of their organization and are enforcing security measures. [10, p. 169.] Bulgurcu et al. defined information security awareness as employees' general knowledge about information security and their understanding of the information security policy of their organization. General information security awareness is defined as employees' overall knowledge and understanding of potential issues related to information security and their ramifications. [11, p. 532.] In this context information security awareness consists of two main areas, firstly, general information security awareness and secondly, knowledge of information security policies and strategies. [12, p. 54.]

3.3. Information security awareness program

Many international IT security standards refer to the implementation of an awareness program as a requirement for getting certification, such as ISO 27001, COBIT, or ISO 9001: 2000.

Concerning information security awareness programs, previous studies -instead of the definition-, focused on the different aspects and purposes of the programs.

Wilson and Hash from NIST (National Institute of Standards and Technology) in their article define security awareness as follows: "Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more normal, having a goal of building knowledge and skills to facilitate the job performance." [13, pp. 8-9.]

Prah, Otchere and Opan –following Chen et al. [14]-, state that "security awareness programs provide users adequate knowledge to evaluate adverse consequences of security problems and take the appropriate actions to prevent and correct security breaches". Thus, information security awareness programs can be used by organizations to make their employees conscious of the security threats that could affect them and how those can be mitigated with security measures. The programs' most important goal is to positively affect the behavior and attitudes of employees towards information security. [8, p. 62.]

Based on the various approaches, security awareness can be described as a continuous effort of raising stakeholders' attention towards information security and its importance, stimulating security-oriented behaviors [15] [16] [17] [18], and ideally inducing stakeholders' compliance to security policies and guidelines. [19, p. 4.] [20]

4. Building an effective Information Security Awareness Program

4.1. Effectiveness

As we can see, numerous studies deal with information security awareness programs from different perspectives. Most of the studies agree that positive influences on users' knowledge, attitudes and behaviors mitigate the impact of security threats and risks the organizations face. Consequently, carefully designed security awareness programs can be effective and successful. [11, p. 523.] [8, p. 63.] [21, p. 2] [22, p. 3.] [23] [24, p. 19.] [25, p. 174.] [26] [27] [28] [29, p. 115.] The knowledge of employees and their willingness to use that knowledge (their attitude) will impact their behavior. As

employees become more security-conscious, the objectives of the information security program are realized, and security risks mitigated. Information security programs fulfilling these requirements can be considered as effective [8, p. 64.] leading to improved security culture of the organization.

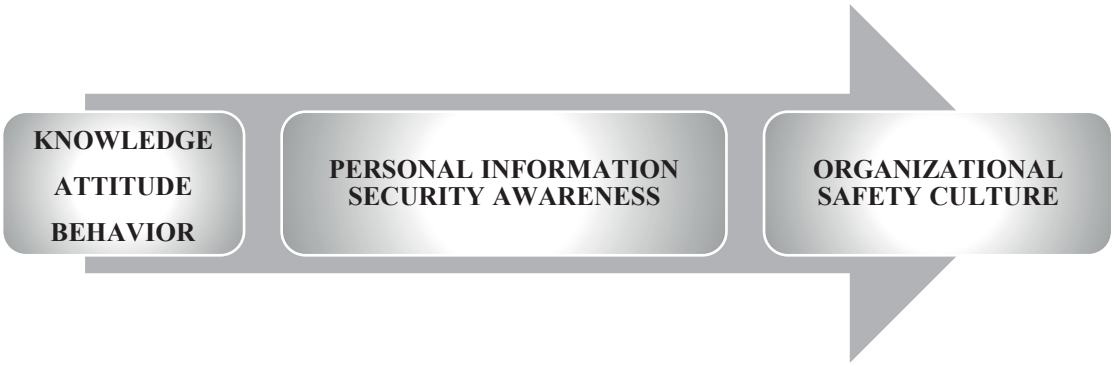

Figure 1: Security awareness

Some researchers have maintained that educating users is futile mainly because it is believed to be difficult to teach users complex security issues and because security is seen as a low priority issue by users and will not pay enough attention to it. [26, p. 3.] The Ernst & Young security survey states that „Many current security trainings and awareness programs are not working as well as they could be". [30]

In fact, numerous studies confirm the difficulties of influencing (the human) behavior and changing (the human) attitude.

The above mentioned issues raise the question, how should an effective Information Security Awareness Program be designed to most effectively influence and improve the user's knowledge, attitude and behavior towards information security and make positive changes in the security culture of an organization?

4.2. Designing an effective Security Awareness Program

According to Wilson and Hash from NIST, there are three major steps in the development of an IT security awareness and training program: designing the program (including the development of the IT security awareness and training program plan), developing the awareness and training material, and implementing the program. „Awareness and training programs must be designed with the organization mission in mind. It is important that the awareness and training program supports the business needs of the organization and be relevant to the organization's culture and IT architecture. The most successful programs are those that users feel are relevant to the subject matter and issues presented." [13, p. 11.]

David Lacey also states that the first step of developing an effective security program is to identify the requirements and the key problem areas, analyze the root causes and develop the programs that indicate corrective actions. [31]

Regarding to relevant studies and best practices, I could set up a model of the key elements of the implementation and the most important five steps to ensure the success of security awareness programs and to help organizations to design their own specific program.

Figure 2: The key elements of the implementation of security awareness programs

I. First, the target group and the program's target are chosen and all relevant information concerning that target is collected [19, p. 6.] [22, p. 21.]
   a) about the organization: public or private sector, the main types of data in organization, the long-term and short-term goals of the organization's strategy;
   b) about the key development areas of information security: identifying the types of threats, vulnerabilities, risks and incidents and their roots;
   c) about the human factors of the organization: the number of employees, fluctuation; for which employee group the program is organized: their age, job descriptions and their level of security awareness.

II. Top management's commitment and resources allocated to awareness: support provided by top management throughout the security awareness initiative, including them acting as role models for all stakeholders; ensure the needed financial, human and other resources required for awareness implementation. [19] [27, p. 11.] [32]

III. Development of the Information Security Program plan:
   a) setting up an awareness project management: formal objectives, milestones and resources should be identified [19] [18] [17]; security policies and procedures that ultimately enhance security awareness implementation [19, p. 7.]; [11, p. 524.] [22, p. 34.] [26, p. 12.] [33, p. 10.] [27, p. 6.] [15] [16]
   b) developing the training material with respect to the target group;
   c) choosing methods and communication channels by focusing on the organizational and human characteristics;
   d) scheduling.

IV. Implementing the program

V. Adjustment of the program based on experience and feedback.

4.3. Development of the Information Security Program plan

In order to make the program able to enhance the knowledge, and change attitudes and behaviors of participants, it is necessary to give the right information to the right person in the right form at the right time.

4.3.1. Developing the training material with respect to the target group – The right information to the right person

Organizations have to highlight and emphasize to employees the interventions or precautions that are necessary to identify and verify an attack before it takes place. „Employees also need to be more aware of how to identify and verify if the person they are dealing with is a social engineer." The training material ensures that employees are updated on recent types of social engineering attacks. [27, p. 6.]

The message of the program needs to be clear, meaningful, personal, memorable and contextualized. The specific, real-life examples and evidence can leave a lasting impression. The programs are more likely to be successful if the users feel that the subject matters and issues presented are relevant to their own needs. [22, p. 32.] [26, p. 5.]

At the same time, if the program and the message are too difficult to use and there are many ambiguous warnings or complicated advice, the users will eventually make mistakes and avoid security altogether. [21, p. 3.] The language and the communication should be understandable, visible and should avoid jargon and technical terminology. The program must be easy to use for all users on each level. [22, p. 4.] [19]

It is very important to use marketing-oriented messages. The basic persuasion techniques include: fear, humor, expertise, repetition, intensity and scientific evidence to seize attention, to establish credibility and trust, and to motivate action. [21, p. 5.] [19] [15] [18] [17]

4.3.2. Choice of methods and communication channels by focusing on organizational and human characteristics – The right information in the right form

The information security message can be delivered with the use of different methods and communication channels.

Promoting information security often creates conflicts with the established work practices. „Information security procedures sometimes may be opposite to efficiency, usability and functionally making users unwilling to follow them and adopt awareness propositions." [19, p. 6.] Security awareness methods should pay attention to minimize difficulties caused to work functionality and efficiency and try to create a balance in the „Security, Functionality and Usability Triangle". [19, pp. 6,7.] [21, p. 4.]

Aldawood and Skinner state that the traditional training methods, including onsite trainings and awareness camps, screensavers, posters, manual reminders and online courses, are boring and tedious, leading to limited success. These methods tend to be very general and sometimes do not focus on the main objective of making staff remember the major manipulation techniques of hackers. [33, p. 7.] „These traditional methods alone do not create sufficient safe culture among staff." [34] Modern training methods, involving real-life simulation scenarios, interactive games, virtual labs, themed

awareness videos and modules, aim to provide awareness of social engineering and of how the social engineers actually perform an attack. [33, p. 6.] [29, pp. 113-115.] [25, p. 174.]

Szász and Kiss confirm the efficiency of modern methods: „It has been demonstrated that the educational method supported by decrypter programs that facilitate student activity had a significantly greater impact on the students' information security attitudes, practices, and awareness than those methods applying only video demonstrations." [35] Scholefield and Shepherd conclude that gamification and gamification techniques were useful methods of raising security awareness and participants enjoyed playing these types of applications and suggested that they increased their knowledge on password security. [36]

Besides these methods we can use many communication channels including formal and informal meetings with groups of employees, formal and informal one-to-one communications, official correspondence such as letters, office orders, e-mails, telephone conversations, communication through discussion groups or chatting with individuals via internet. According to Rehman et al. the face-to-face communication is the most effective medium. The richest of these forms of communication is the one-to-one interaction. [37, pp. 20.,21.] We can also use the corporate events (conferences, seminars, internal company meetings, road shows) as they can have a positive security influence to the persuasion process. We should attempt to use such methods as campaigns, newsletters, screensavers, DVDs, PR films or videos, trinkets, brochures and flyers to raise users' awareness. [8, p. 63.] [22, pp. 32.,33.]

In a nutshell, more categorized trainings, methods and communicational channels are needed to develop the knowledge base, the adequate attitude and the expected behavior against threats. The choice of method depends on each organization, their objective and target audience. [8, p. 63.]

4.3.3. Scheduling - The right information at the right time

Information security needs to be focused on the goal of becoming effortless. Whenever possible, detailed aspects of day-to-day operational computer security should not be difficult or greatly time-consuming for the end user, meaning that the awareness program and its methods should be made easier for users. [22, p. 4.]

It is important for employees to be periodically educated. Many scholars confirm that it is critical to keep staff prepared to practice their duties and behave safely in the workplace. [27, p. 6.] [38, p. 5.] [24, p. 26.] Organizations need to educate staff about common manipulative methods used by hackers and dangerous actions, regardless of their job. It is necessary to constantly remind staff of how their vulnerability can cause harm to the organization. [39, p. 6.] Training or other awareness methods should be used regularly in order to prevent information security awareness from decreasing among employees.

5. Conclusion

It is important to keep in mind the human factor, as the employee is the first line of defense against security threats and risks. Since users are the first targets of social engineering attacks, security awareness programs are one of the greatest defenses.

This study has expanded the understanding of information security and security awareness from various perspectives. In order to enable organizations to implement a successful security awareness

program, the main factors of effectiveness have been analyzed as a starting point. The conclusion is that there is a positive relationship between users' knowledge, attitude and their self-reported behavior, so awareness programs should positively affect these three components towards information security.

This paper also presents an overview on how to develop and build an effective information security awareness program. To achieve that goal, the most important concepts have been analyzed and then the five key elements of the implementation have been identified. To explore implementation challenges, the main areas of challenges have been collected and analyzed. The importance of clear, understandable, marketing-oriented message, adequate communication without jargon and technical terminology and application of persuasion techniques have also been examined as essential elements of a successful program.

One of the aims of this research was to provide practical help for practitioners developing their awareness program with a collection and evaluation of different methods and communication channels and a comparison of traditional trainings with modern programs.

The conclusion is that each organization should develop and implement an awareness program tailored to its own specificities and needs, using a variety of communication channels and tools to raise employees' awareness and build an adequate cyber security culture.

6. References

[1] CHANTLER, A. N. and BROADHURST, R., „Social engineering and crime prevention in cyberspace," *SSRN Electronic Journal,* p. 23, 2008.

[2] DEÁK, V., „A social engineering humán alapú támadási technikái," *Biztonságpolitika,* p. 11, 2017.

[3] BÁNYÁSZ, P., „Social engineering and social media," *Nemzetbiztonsági Szemle 6. évf. 1. szám,* pp. 59-77., 2018.

[4] DEÁK, V., „A számítógép alapú social engineer támadási technikák," *Biztonságpolitika,* p. 9, 2017.

[5] ALDAWOOD, H. and SKINNER, G., „Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues," *Future Internet 11(3),* p. 16, 2019.

[6] KRUGER, H. A. and KEARNEY, W. D., „A prototype for assessing information security," *Computers & Security 25(4),* pp. 289-296., 2006.

[7] AJP-3.10 ALLIED JOINT DOCTRINE FOR INFORMATION OPERATIONS, NATO/PfP UNCLASSIFIED publication. 2009. Available: https://info.publicintelligence.net/NATO-IO.pdf [Accessed: January 12, 2020]

[8] PRAH, A. N. W., OTCHERE, A. A. and OPAN, K. E., „The Perceived Effectiveness of Information Security Awareness," *Information and Knowledge Management Vol.6, No.7.,* pp. 62-73., 2016.

[9] SHAW, R. S., CHEN, C. C., HARRIS, A. L. and HUANG, H.-J., „The impact of information richness on information security awareness training effectiveness," *Computer & Education 52.,* pp. 92-100., 2009.

[10] NEMESLAKI, A. and SASVÁRI, P., „Az információbiztonság-tudatosság empirikus vizsgálata a magyar üzleti és közszférában," *Infokommunikáció és Jog, 2014/4. (60.),* pp. 169-177.

[11] BULGURCU, B., CAVUSOGLU, H. and BENBASAT, I., „Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly Vol. 43. No. 3.,* pp. 523-548., 2010.

[12] ILLÉSSY, M., NEMESLAKI, A. and SOM, Z., „Elektronikus információbiztonság-tudatosság a magyar közigazgatásban," *Információs Társadalom ,* pp. 52-73., 2014/1.

[13] WILSON, M. and HASH, J., Building an Information Technology Security Awareness and Training Program, National Institute os Standards and Technology, 2003., p. 70.

[14] CHEN, C. C. and MEDLIN, D. B., „A cross-cultural investigation of situational information security awareness programs," *Information Management & Computer Security 16(4),* pp. 360-376., 2008.

[15] PELTIER, T. R., „Implementing an Information Security Awareness Program.," *Information Systems Security, 14 (2),* pp. 37- 48., 2005.

[16] ENISA, „A NEW USERS' GUIDE: HOW TO RAISE INFORMATION SECURITY AWARENESS," 2008. [Online]. Available: https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide. [Accessed: January 10, 2020].

[17] HANSCHE, S., „Designing a Security Awareness Program: Part I.," *Information Systems Security, 9(6),* pp. 14-23., 2001.

[18] MAEYER, D. D., „Setting up an Effective Information Security Awareness Programme," in *In: ISSE/SECURE 2007 Securing Electronic Business Processes Highlights of the Information Security Solutions Europe/SECURE 2007 Conference (part 1),*, 2007.

[19] TSOHOU, A., KARYDA, M. and EL-HADDADEH, R., „Implementation challenges for information security awareness initiatives in e-government," in *European Conference on Information Systems*, 2012.

[20] SIPONEN, M., „A conceptual foundation for organizational information security awareness," *Information Management & Computer Security, 8 (1),* pp. 31-41., 2000.

[21] BADA, M., SASSE, A. M. and NURSE, J. R. C., „Cyber Security Awareness Campaigns: Why do they fail to change behaviour?," in *International Conference on Cyber Security for Sustainable Society*, 2015.

[22] PARSON, K., MCCORMAC, A., BUTAVICIUS, M. and FERGUSON, L., *Human factors and information security: Individual, culture and security environment,* Edinburgh: Published by Command, Control, Communications and Intelligence Division DSTO Defence Science and Technology Organisation, 2010, p. 54.

[23] TSOHOU, A., KARYDA, M. and KOKOLAKIS, S., „ Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs," *Computers & Security 52.,* pp. 128-141., 2015.

[24] PATTINSON, M., JERRAM, C., PARSONS, K., MCCORMAC, A. and BUTAVICIUS, M., „Why do some people manage phishing e-mails better than others?," *Information Management & Computer Security, Vol. 20 No. 1,* pp. 18-28., 2012.

[25] PARSON, K., MCCORMAC, A., BUTAVICIUS, M., PATTINSON, M. and JERRAN, C., „Determing employee awareness using the HumanAspects of Information Security Questionnaire (HAIS-Q)," *Computers & Security 42,* pp. 165-176., 2014.

[26] STEPHANOU, T. and DAGADA, R., „The impact of security awareness training on information security behaviour: The case for further research," in *Conference paper: Proceedings of the ISSA 2008 Innovative Minds Conference, ISSA 2008, Gauteng Region (Johannesburg),*, 2008.

[27] ALDAWOOD, H. and SKINNER, G., „ Contemporary cyber security social engineering solutions, measures, policies, tools and applications: A critical appraisal," *International Journal of Security (IJS), Volume (10) : Issue (1),* p. 15, 2019.

[28] ALDAWOOD, H. and SKINNER, G., „A critical appraisal of contemporary cyber security social engineering solutions: measures, policies, tools and applications;, p. 6," in *Conference paper: 2018 26th International Conference on Systems Engineering (ICSEng)*, 2018.

[29] ALDAWOOD, H. and SKINNER, G., „Challenges of implementing training and awareness programs targeting cyber security social engineering," in *Conference paper: 2019 Cybersecurity and Cyberforensics Conference (CCC),*, Melbourne, Australia, 2019.

[30] ERNST & YOUNG (2010), „"12th annual global information security survey: Outpacing change",," [Online]. Available: http://www.ey.hu/TW/en/Issues/Managing-risk/Information-security-and-privacy. [Accessed: December 12, 2019].

[31] LACEY, D., Managing the human factor in information security - How to Win Over Staff and Influence Business Managers, 2009., p. 398.

[32] KOLLÁR, CS, „Az információbiztonság-tudatosság fejlesztése a (felső)vezetők körében," *Magyar Coachszemle V. évfolyam 3. szám ,* pp. 35-50., 2016.

[33] ALDAWOOD, H. and SKINNER, G., „Reviewing Cyber Security Social Engineering Training and Awareness Programs—Pitfalls and Ongoing Issues, p.16," *Future Internet 2019, 11(3), 73,,* p. 16, 2019.

[34] ABAWAJY, J., „User preference of cyber security awareness delivery methods," *Behaviour & Information Technology, 2014. Vol. 33, No. 3, ,* p. 236–247.

[35] SZÁSZ, A. and KISS, G., „Jelszóvisszafejtő programok oktatási célú felhasználása és hatásuk az információbiztonsági tudatosságra," *Információs Társadalom, XVIII. évf. (2018) 3–4. szám,,* p. 82–104.

[36] SCHOLEFIELD, S. and SHEPHERD, L. A., *Gamification Techniques for Raising Cyber Security Awareness,* Workshop on Serious Games for Cyber Security- Heriot-Watt University, Edinburgh, United Kingdom, 2019., p. 15.

[37] REHMAN, S. U. and MAROUF, L., „Communication Channels and Employee Characteristics: An Investigation," *Singapore Journal of Library & Information Management, Volume 37, 2008,,* pp. 13-43.

[38] ALOUL, A. F., „Information security awareness in UAE: A survey paper; Conference paper: IEEE International Conference on Internet Technology and Secured Transactions (ICITST)," 2010.

[39] GREAVU-SERBAN, V. and SERBAN, O., „Social engineering a general approach," *Informatica Economica, vol. 18, no. 2,* pp. 5-14., 2014.