ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 7 Number 3 (March)
http://doi.org/10.9770/jesi.2020.7.3(26)

Publisher
http://jssidoi.org/esc/home

TRAINING IN SHAPING EMPLOYEE INFORMATION SECURITY AWARENESS

Tomasz Stefaniuk

Siedlce University of Natural Sciences and Humanities, Faculty of Social Sciences, ul. Konarskiego 2 08-110 Siedlce Poland

E-mail: tomasz.stefaniuk@uph.edu.pl

Received 19 September 2019; accepted 15 December 2019; published 30 March 2020

Abstract. The purpose of this paper is to present the effectiveness of training in the development of employee awareness in the area of information security. Two kinds of primary research were carried out: surveys conducted among employees of various organizations, the essence of which involved a comparison of the awareness level in terms of security among people who had participated and those who had not participated in information security training; and a comparative analysis of results of an audit of information security awareness conducted among employees of a large organization before and after conveying information security training. Research results showed significant effectiveness of training as a method not only of information security knowledge extension but also, and most importantly, one that has a significant impact on actual behaviors of employees in the studied area. Due to the fact that the greatest gap in security measures involves the lack of employee awareness, and because training is an effective method of shaping the said awareness, organizations should develop and implement an adequate training program raising the level of employee awareness in terms of information security. It should be remembered that the program cannot be a one-off event but rather a cyclical one. While the importance of awareness in information security is well described in the subject literature, there is a shortage of publications, which show a direct influence of training on employees' level of knowledge and behaviors in terms of information security. This paper, in an interesting, dual way, points to an actual impact of training both on expanding knowledge and on behaviors in terms of information security.

Keywords: information security; employee training; information security awareness (ISA)

Reference to this paper should be made as follows: Stefaniuk, T. 2020. Training in shaping employee information security awareness. *Entrepreneurship and Sustainability Issues*, 7(3), 1832-1846. https://doi.org/10.9770/jesi.2020.7.3(26)

JEL Classifications: M12, M15, M53

1. Introduction

In the contemporary electronic knowledge-based economy, information has become a precious resource. Due to its value, it is a desirable good that a lot of institutions and private individuals try to obtain in an illegal way. An analysis of media reports concerning cybersecurity in recent years presents a truly gloomy picture of the contemporary world, where information faces great vulnerability to theft or destruction. Every year, the number

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 7 Number 3 (March)
http://doi.org/10.9770/jesi.2020.7.3(26)

of cyber-attacks observed throughout the world is rising by close to 50%, as shown in the PwC report "Risk management in cyberspace" (PWC, 2015).

On the other hand, for many years now all research devoted to information security has been pointing to man as the main perpetrator of incidents threatening information security. It needs to be noted that as many as 70% of all information security abuse cases in Poland were committed by organizations' employees (of which 48% by current employees and 22% by former employees (The Global State of Information Security® Survey 2015, PWC, p. 16).

Internal threats are considered more dangerous than external ones as their consequences lead to much greater damage and complications (Jabłoński, Mielus, 2010, p. 31).

It is people who are the weakest link in the information security system in organizations, actions directed at employees and subcontractors are crucial, as pointed out by a number of authors who rightfully emphasize that the mere technical measures are no longer sufficient to ensure information security in an organization (Vroom and Solms, 2004, Schultz, 2005; McCormac et al., 2017; Chehabeddine, Tvaronavičienė, 2020).

The above thesis is confirmed by a global information security research carried out by EY (2017) which shows that the greater blank in security measures involves the lack of employee awareness (2013 - 53%, 2014 - 57%, 2015 - 44%, 2016 - 55%) (EY, 2017). Therefore, developing appropriate employee behaviors in an organization plays no lesser role in the organization's information security than any other technical measure (Jabłoński, Mielus, 2010, Kraemer et al., 2009).

As employee training is one of the ways to develop employee awareness in terms of information security, the aim of this paper is to specify the effectiveness of training in terms of building employee awareness in the sphere of information security.

2. Review of theory on the development of employee awareness in the sphere of information security

There is no single universal definition of information security awareness in the literature, yet two trends in interpreting this notion can be observed. Some authors bring down information security awareness to having knowledge about information security threats and ways to prevent them, i.a.: Banerjee and Pandey (2010); Banerjee et al. (2013); Chen et al. (2006); ENISA (2006); Okenyi and Owen 2007); Lim et al. (2010). In this meaning, the awareness level may be specified by the level of one's knowledge and skill.

The other group of researchers points to the dimension of action. Therefore, information security awareness is the degree to which an individual (employee) not only understands the significance of IT security and knows IT security levels adequate to the organization and their individual security-related responsibilities but also acts accordingly. Such a position is adopted by i.a.: Shaw et al. (2009); ISF Standard (2007); Tsohou et al. (2015), Rotvold and Braathen (2008); Rastogi and von Solms (2012); Hellqvist et al. (2013).

As a rule, the second approach grades awareness levels making it possible to create models of measuring information security more precisely. Having information security knowledge is the initial (lowest) degree of awareness. However, the mere knowledge is not worth much if it does not imply adequate attitudes (belief that certain security measures must be taken and willingness to act). The final, highest expression of awareness involves adequate employee behavior (Figure 1).

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 7 Number 3 (March)
http://doi.org/10.9770/jesi.2020.7.3(26)

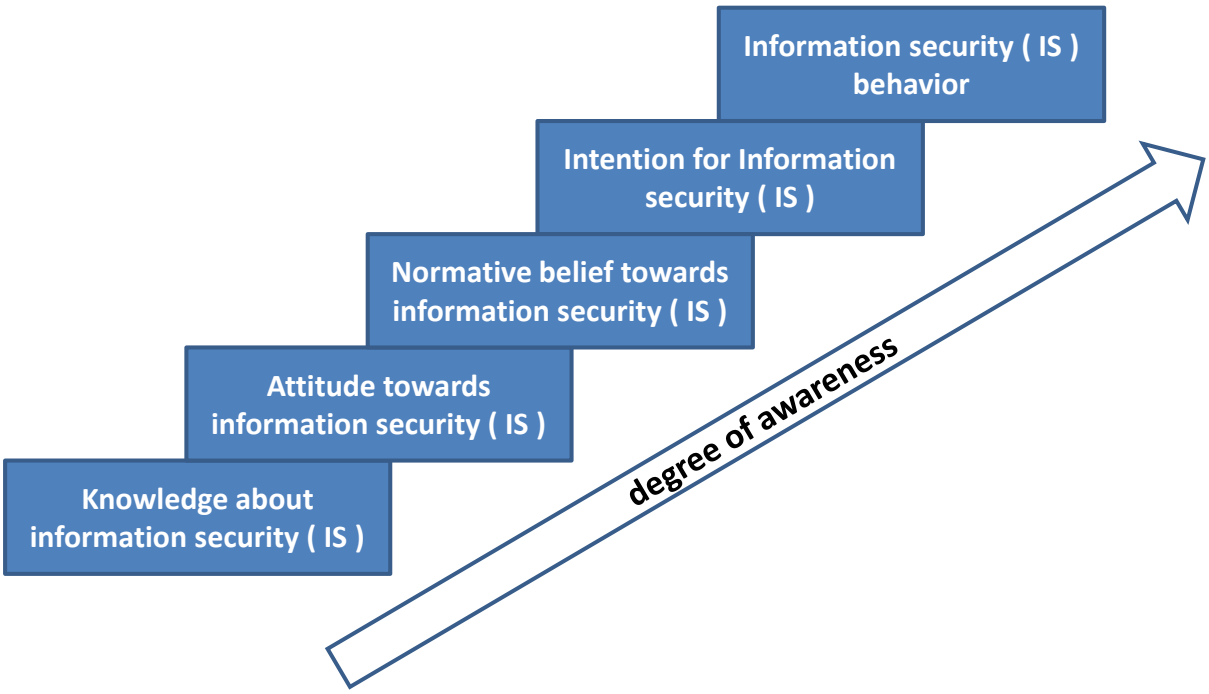

Fig. 1. Five-step ladder model for measuring information security awareness.
Source: Khan et al. (2011, p. 10864)

According to Data Security Standard (PCI 2014), directing the provision of appropriate materials to appropriate recipients in a swift and effective way is the key to effective raising of information security awareness. Both on the theoretical and the practical grounds, numerous methods of building information security awareness can be identified: traditional as well as ICT technology-based. The most frequently employed methods include (PCI, 2016, p. 5; Chmura 2017, pp. 80-86; Khan et al., 2011):

1. Classroom training (at a work place or in an external center). The main purpose involves providing an employee with a knowledge compendium (Kopier 2011) related to information security (policy and procedures in force in the organization, changes etc.) in a quick and effective manner.
2. Group discussion. It is a meeting of 15-20 people during which the participants fully draw from sharing knowledge and experience. There is no one-way communication in there. Information security-related issues are selected one by one and discussed, and all participants have equal opportunities to explain their points of view (Albrechsten and Hovden, 2010).
3. Newsletters. They are aimed at strengthening information security programs. They can be both in a paper and electronic form. They provide an opportunity to send numerous messages at the same time.
4. Video games – they stimulate information security knowledge, combine fun and training. They have significant impact on the change of the user's attitude, however they are not the best source of provision of detailed information on one's information security policy.
5. Video clips. The formula of this method makes it possible for the participants to learn whenever or for how long they wish as no time restrictions are imposed. However, they do not allow instructor-training participant interaction.
6. Poster campaigns. Placing posters in shared areas is aimed at drawing greater attention in a slogan-like way to specific steps (behaviors) that need to be taken in order to improve security.
7. CBT – Computer-based training.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 7 Number 3 (March)
http://doi.org/10.9770/jesi.2020.7.3(26)

8. Internet methods which include:
    a. dedicated websites, e.g. www.pcisecuritystandards.org,
    b. e-mail,
    c. blogs,
    d. animations and multimedia,
    e. social media,
    f. discussion groups,
    g. intranet.

Each of the above methods has their own virtues and flaws. For instance, electronic notifications are easier to read but also easier to ignore by busy staff. On the other hand, security-related events which require active participation of staff are exceptionally effective.

According to research carried out by B. Khan et al. (2011), the following feature highest effectiveness: group discussion and classroom training (5 and 4 in the five-point Likert scale, respectively). Effectiveness of training as a method of enhancing knowledge on user security is confirmed by literature review (Chmura 2017).

In turn, according to the PCI Standard (2014), the effectiveness of training in raising awareness is determined by the level of engagement and, indirectly, also by the size of the group of recipients taking part in it. Recipient engagement, implemented by scenario-based activities, solving case studies or focused discussion help ensure that the concepts are understood and memorized. Group size is correlated with engagement levels: the larger the group, the greater the risk that the content is not effectively communicated since individuals may lose focus on the presented material.
The communication channel used should match the audience receiving the training content, the type of content, as well as the content itself (PCI 2015). In turn, conducting security awareness training by way of many communication channels ensures that employees acquire and remember the presented information better.

As rightly noted by Ahmad et al., (2012), Balcerek et al., (2012) and Desman (2013), a properly planned and implemented ISA program fills the gap between end users and technology. As a result, ISA programs are becoming, perforce, a norm for organizational protection of end-user risk (Peltier, 2013; Tsohou et al. 2015; Vroom & Solms, 2004).

A number of international standards specify the implementation of an ISA program as a preliminary condition for constructing an effective system of information security management, for instance:

- *ISO/IEC 27001* (PN-EN ISO/IEC 27001:2017),
- COBIT (IT 2007),
- Payment Card Industries – Data security (ENISA 2007)
- ISO 9001: 2000 (ENISA 2007).

Thus, if an organization or company wishes to obtain a certificate in one of these standards they must first implement a security awareness raising program.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 7 Number 3 (March)
http://doi.org/10.9770/jesi.2020.7.3(26)

3. Research objective and methodology

Dual primary research was carried out (Figure 2):
1. Between June 2018 and February 2019, a survey was carried out among 260 employees of various organizations (aged between 20 and 65), who were willing to improve their competences in terms of personal data protection. Fifty-five percent of them were men and forty-five percent were women. They represented organizations of various sizes: small organizations, employing fewer than 20 staff (28.8% of respondents), and organizations with over 200 employees (34% of respondents). The essence of this research involves a comparison of the level of awareness in terms of security among persons who have and those who have not participated in an information security training. The existence of a relationship between knowledge and actual behaviors of employees in the sphere of information security and participation in data security training was verified by means of the $\chi 2$ test of independence according to formula (1).

$$\chi^2 = \sum_{i=1}^{n} \frac{(O_i - E_i)^2}{E_i} \quad (1)$$

Where:
O – observed value, E – expected value

Expected values were specified according to the following formula (2),:

$$E_{expected} = \frac{(sum\ of\ row)\ (sum\ of\ column)}{(total\ sum)} \quad (2)$$

In order to investigate the impact of training on information security awareness Cramer's V contingency coefficient (3) was also calculated.

$$V = \sqrt{\frac{\chi^2}{n(m-1)}} \quad (3)$$

2. A comparative analysis of results of an information security audit conducted among employees of a large organization before and after information security training was carried out.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 7 Number 3 (March)
http://doi.org/10.9770/jesi.2020.7.3(26)

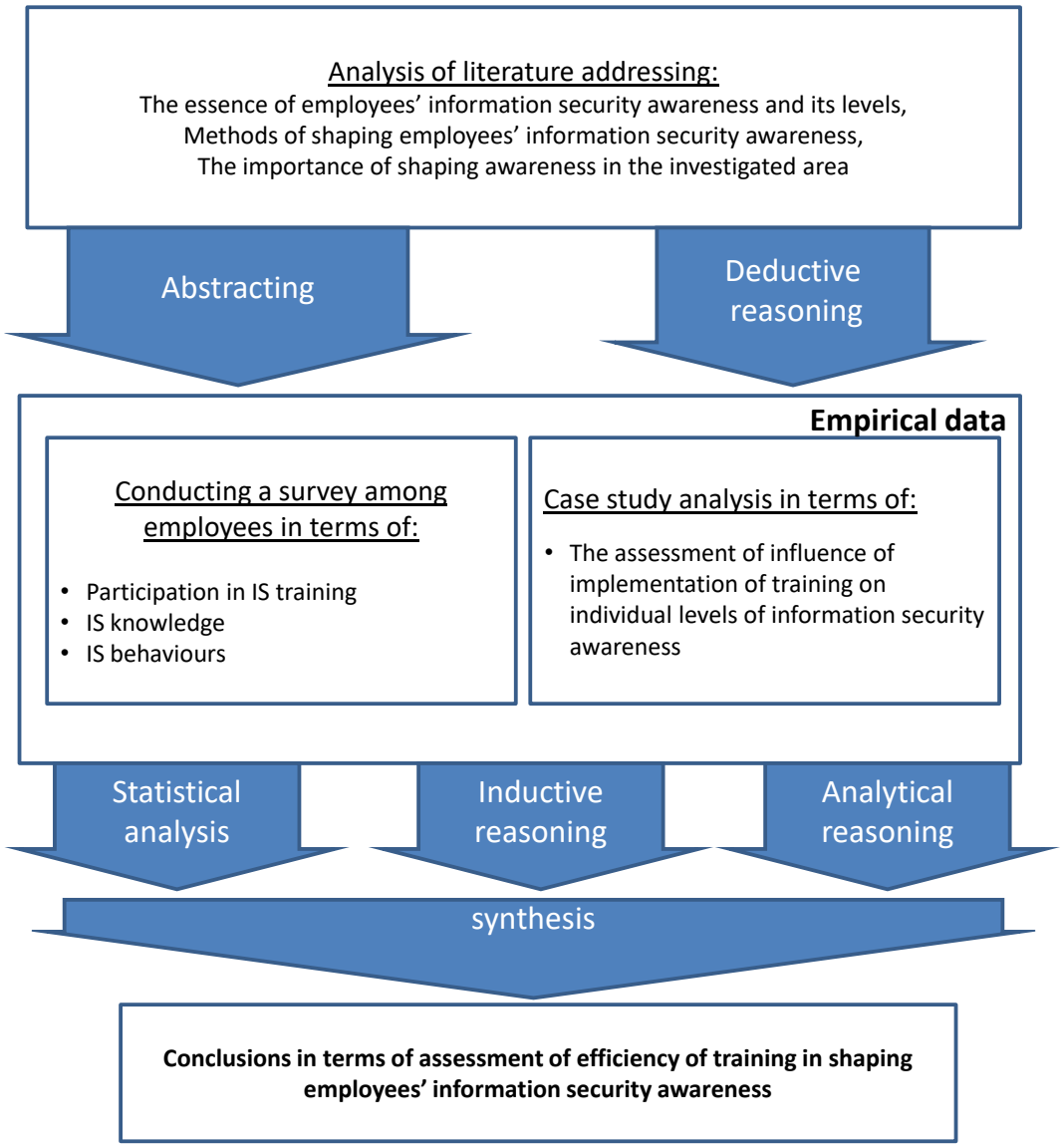

Fig. 2. Applied research process.
Source: author's own compilation

4. Research results

a. Analysis of survey results

When juxtaposing participation in training with the number of people employed in an organization, a marked difference between small companies and the rest of organizations can be observed. Only 20% of employees of small organizations have participated in information security training. Among larger organizations, the percentage of trained people was significantly higher, which was presented in Figure 3. The above trend could have been expected, however such a great discrepancy comes as a major surprise.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 7 Number 3 (March)
http://doi.org/10.9770/jesi.2020.7.3(26)

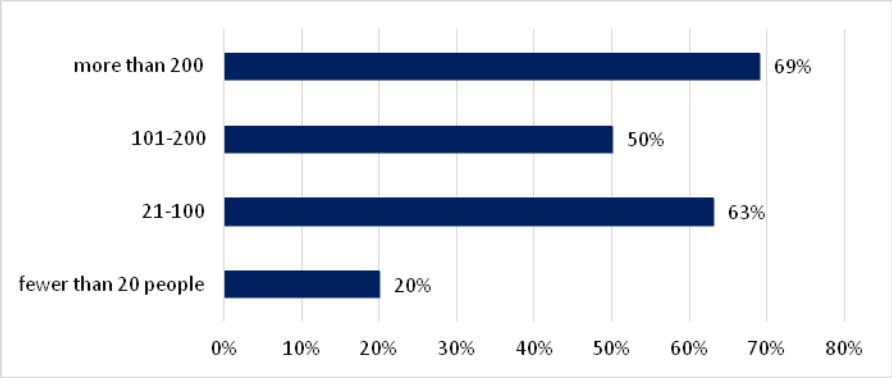

Fig.3. Percentage of people who have participated in information security training from the perspective of the number of people employed in a company.
Source: author's own compilation.

The first element investigated in terms of knowledge in the sphere of information security was familiarity with personal data processing processes. The ability to identify these processes – defining whether a performed activity is compliant with the applicable law or process of personal data processing – is key to the process of protection of this data. It implies the need to meet a number of obligations imposed on the processor in terms of protection of processed data.

As can be noted in Figure 4, persons who have participated in information security training over the last 2 years were able to identify personal data processing processes better than persons who have not taken part in such training.

Only 31% of people who have not participated in training correctly included deleting data as one of personal data processing processes, while in the group of persons who have been trained correct answers were given by 72% of respondents.

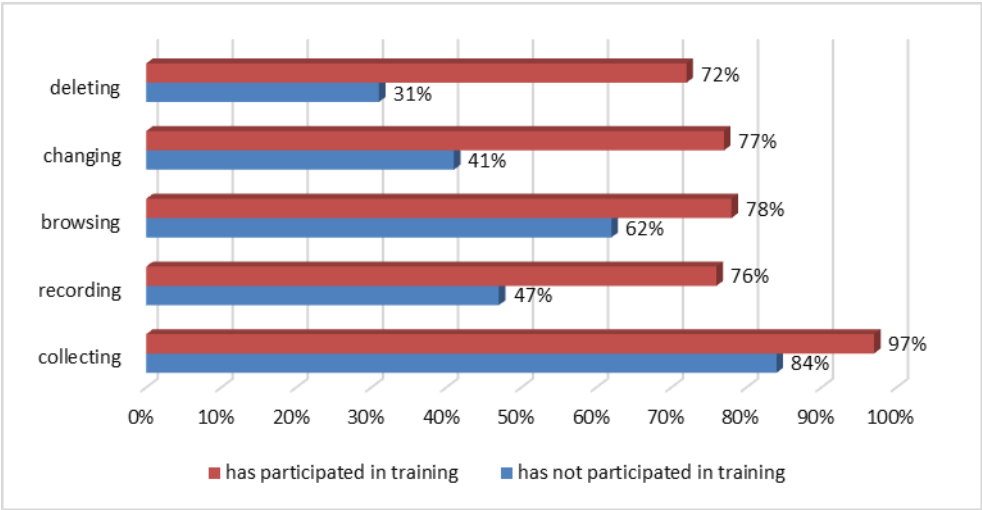

Fig.4. Identification of personal data processing activities by persons who have and those who have not participated in information security training
Source: author's own compilation.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 7 Number 3 (March)
http://doi.org/10.9770/jesi.2020.7.3(26)

The relationship between correct indication of a personal data processing process and participation in information security training was verified by the $\chi 2$ test of independence according to formula (1). In order to investigate the impact of training on information security awareness Cramer's V contingency coefficient (3) was also calculated. Results are presented in Table 1.

Table 1. The relationship between correct indication of a personal data processing process and participation in information security training

Processing process	calculated χ^2	χ^2 for α=0.05	χ^2 for α=0.005	V_{cr}
collecting	8.61	3.84	7.87	0.24
recording	13.33	3.84	7.87	0.30
browsing	4.90	3.84	7.87	0.18
changing	21.32	3.84	7.87	0.37
deleting	25.83	3.84	7.87	0.41

Source: author's own compilation.

As you can see, for the significance level α=0.05 there is a relationship between participation in training and correct identification of all personal data processing processes. With the significance level α=0.005, the above correlation is significant for the processes of collecting, recording, changing and deleting. The specified Cramer's V contingency coefficient shows that the above correlation is moderately strong.

Analogically to the previous question, the difference between persons who have and those who have not participated in information security training could be noted in identification of personal data subject to special protection (the so-called sensitive data). Admissibility of processing special categories of personal data was limited in Article 9 GDPR in relation to regular data since their processing in the assessment of the legislator brings a serious threat to fundamental rights and freedoms. Under the Act of 29 August 1997 on the protection of personal data applicable in Poland before the GDPR, the catalogue of sensitive personal data included information concerning convictions, rulings imposing a penalty and fines, as well as other rulings issued in court or administrative proceedings. Article 9(1) GDPR excludes data on convictions or violations of the law (it does not list them) from the catalogue of sensitive data. Nevertheless, Article 10 GDPR points out that despite the exclusion of (not including) this data from the catalogue of sensitive data their processing must be based on the provision of domestic or Union law. As a consequence, these data are subject to special protection in Poland.
Only 14% of people who have not participated in training correctly pointed to a ruling imposing a penalty and information about fines as an example of sensitive personal data, while in the group of persons who have been trained correct answers were given by 53% of respondents (Fig. 5).

Also in this case the relationship between correct identification of personal data subject to special protection and participation in training was confirmed statistically. The calculated χ^2 value was 30. For the significance level α = 0.005 and df=3, the theoretical value of χ^2 is 12.8. Cramer's V contingency coefficient was 0.44, which evidences a moderate strength of association between correct indication of personal data subject to special protection and participation in data protection training.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 7 Number 3 (March)
http://doi.org/10.9770/jesi.2020.7.3(26)

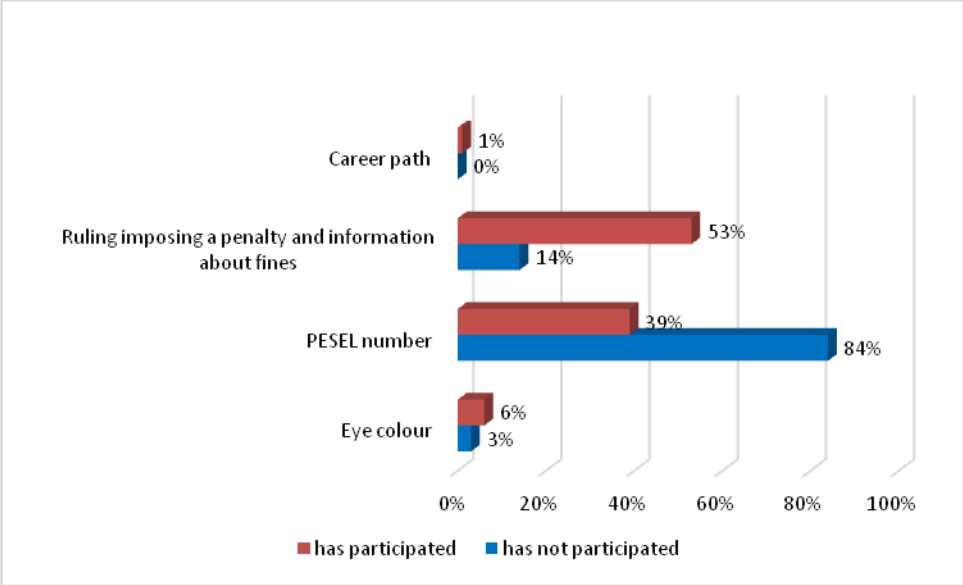

Fig.5. The correctness of indicating personal data subject to special protection among persons who have and those who have not participated in information security training
Source: author's own compilation

An analysis of responses confirmed great significance of training as a method of enhancing knowledge on information security.

Participation in training did not only broaden employee knowledge of information security but it also had a significant impact on actual employee behavior in this sphere.

As an example, one can point to the frequency of changing an email password among persons who have and those who have not participated in training. Almost 40% of employees who have not participated in information security training have not changed their email passwords. In the group of people who have participated in training this percentage is lower by almost a half at 20.4%. On the other hand, people who have participated in training prevail in the group of persons who change their email password, where the difference is more pronounced among those changing their password every 1-3 months. i.e. 16% and 5% respectively (Fig.6).

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 7 Number 3 (March)
http://doi.org/10.9770/jesi.2020.7.3(26)

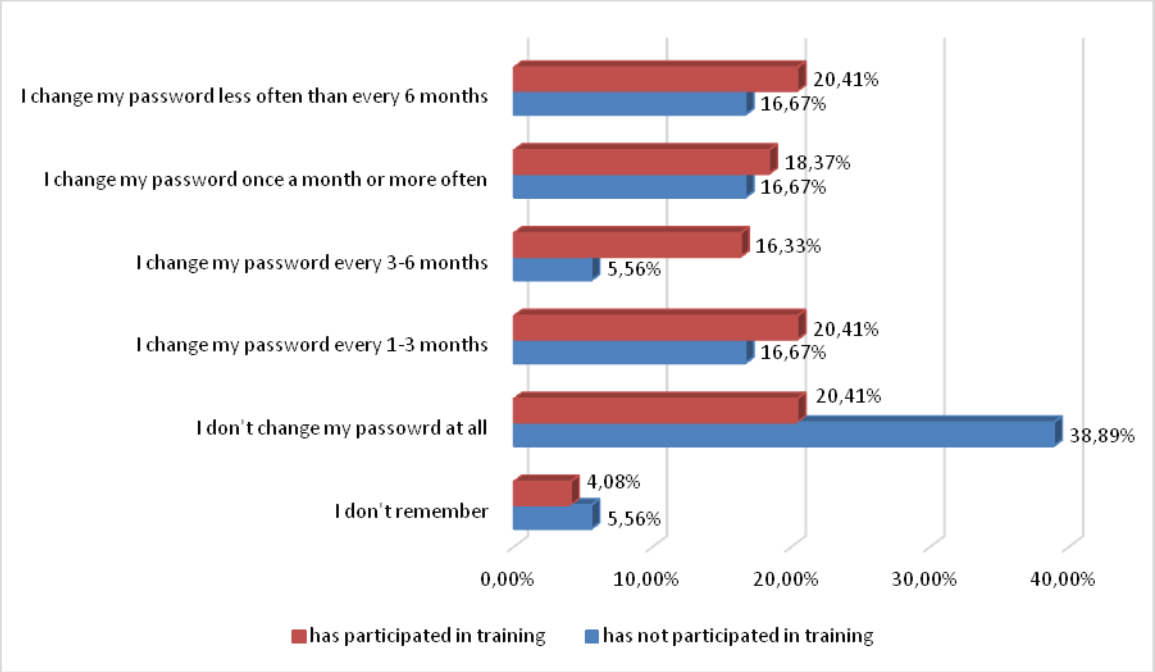

Fig.6. Frequency of email password change among persons who have and those who have not participated in information security training
Source: Author's own compilation

Also in this case the existence of a relationship between the frequency of password change and participation in data security training was verified by the $\chi 2$ test of independence.

The result ($\chi 2=20$ with significance level alfa = 0.005 and df=6) confirmed the existence of such a correlation. Cramer's V contingency coefficient (3) was also calculated. It was 0.36, which testifies to a moderate strength of association between investigated phenomena.

The second analyzed example of existence of a relationship between information security training and actual employee behavior involved having an authority to process personal data among employees declaring that they do process such a category of data. GDPR (Article 29 and 32(4)) imposes an obligation under which each authorized person (e.g. employee) who has access to personal data shall process it solely on instructions from the controller (e.g. employer). Even though the authority does not need to be given in writing, it still needs to be well documented. It can be included under the employee's responsibilities or possibly a separate template may be created.

As demonstrated by Figure 7, only 42% of persons who have not participated in training and who do process personal data have the authority to process it. In the group of persons who have recently participated in information security training, 80% of processors have the authority.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 7 Number 3 (March)
http://doi.org/10.9770/jesi.2020.7.3(26)

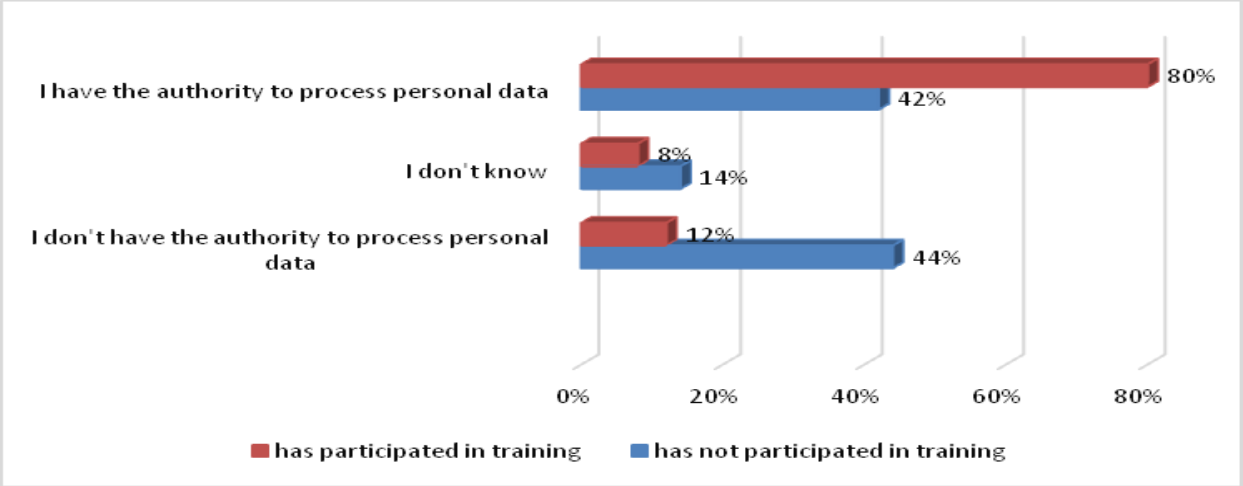

Fig. 7. Having authority to process personal data among employees processing personal data
Source: Author's own compilation

b. Analysis of audit results in organization x

The analysis of results of an audit of information security awareness led to similar conclusions as regards the significance of training as a method for extending knowledge on information security which also has a significant influence on the actual employee IS behavior.

Such an audit was carried out among employees of a large scientific and didactic organization before and after training employees in the area of information security. This study was conducted on 98 employees (10% of total employed).

Comparing results of both audits, a significant increase was observed in both the awareness of the fact that there is an information security management system in the organization (increase by 12%) and the fact of publishing the document "Information security policy" and making it available (increase by 18%).

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 7 Number 3 (March)
http://doi.org/10.9770/jesi.2020.7.3(26)

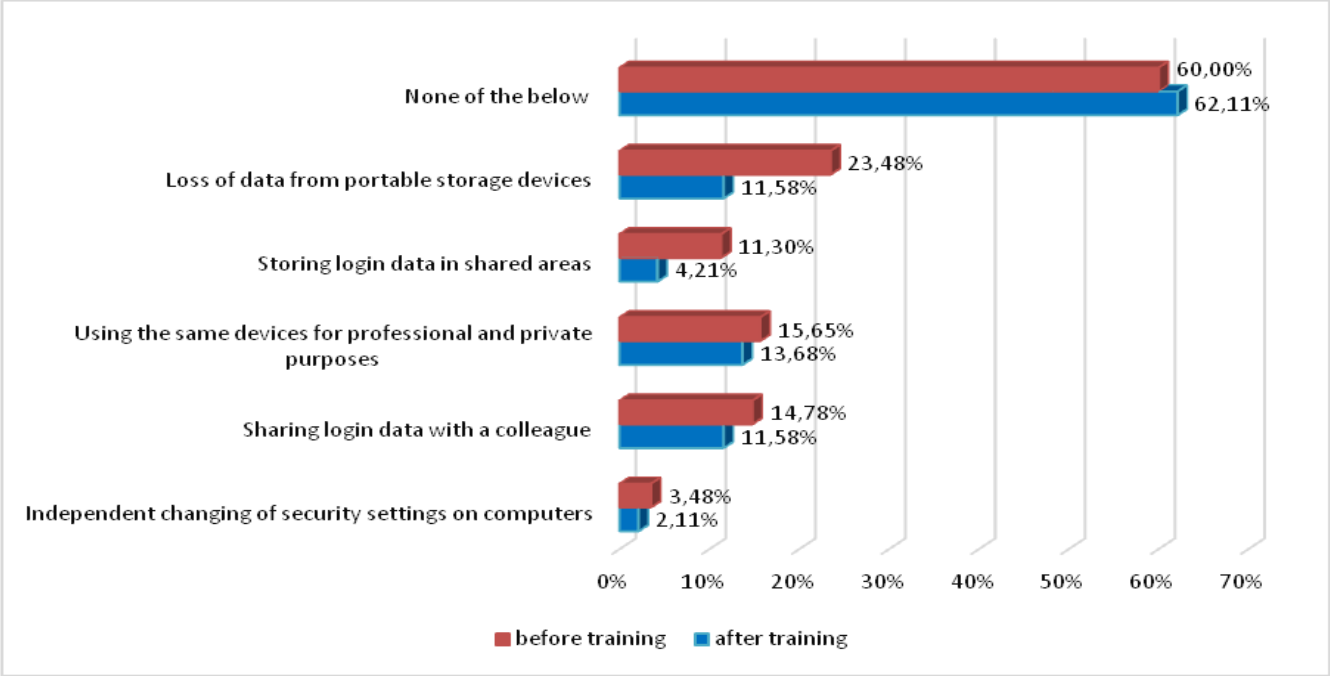

Fig. 8. Negative situations encountered by employees of the audited organization in their work
Source: Author's own compilation

The greatest increase was observed in employees' declarations as to their compliance with the principles and rules of the information security policy. In the study carried out after training, such a response was given by 70% of employees, whereas in the previous audit such a declaration was given by only 38% of employed persons.

However, what is more essential, following training a lower frequency of negative events in the sphere of information security was noted, i.a.: loss of data from portable storage devices – decrease by half from 23.48% to 11.6%, or storing usernames and passwords in shared areas – decrease from 11.3% to 4.21% (Figure 8).

Conclusions

As rightly pointed out by Hadlington (2017), each information security breach incident in an organization is more or less is determined not only by technology but also, and primarily, by people. Employees' improper conduct or lack of action lead to the majority of information security incidents. Therefore, employees' understanding of consequences of their behavior is key to the security of the organization's information and ITC systems.

Training is an effective method of shaping employee awareness in the area of information security. Research results have shown great effectiveness of training as a method of not only improving knowledge of information security, but mainly one that has a significant impact on the actual IS behavior of employees.

In order to minimize the risk of occurrence of information security incidents, organizations are obliged to develop and implement an adequate training program, which boosts the level of employees' awareness in the sphere of information security.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2020 Volume 7 Number 3 (March)
http://doi.org/10.9770/jesi.2020.7.3(26)

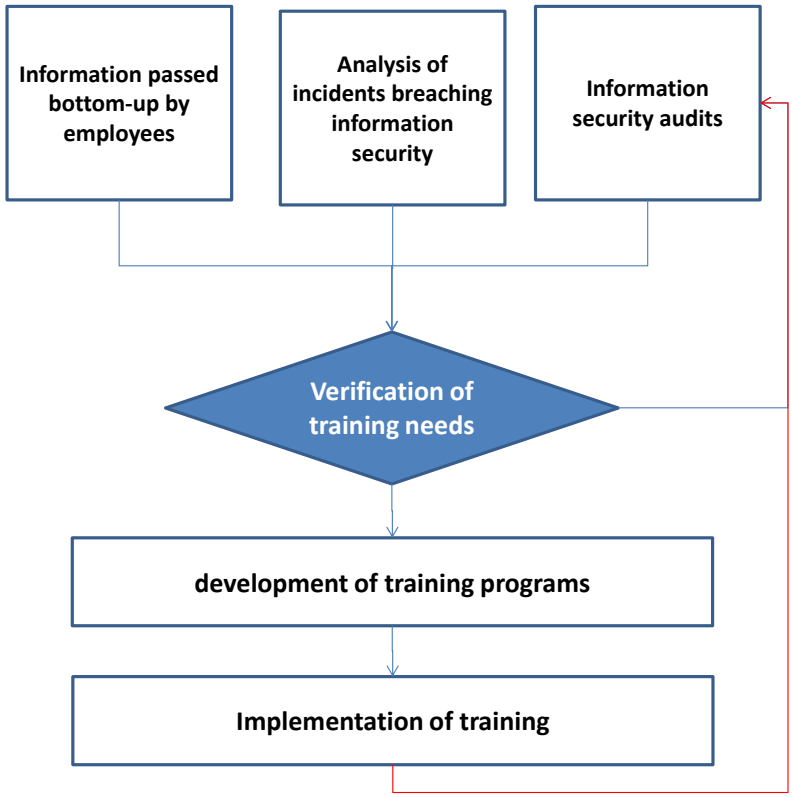

Fig.8. Information security training as a regular activity
Source: Author's own compilation

One needs to bear I mind that this program cannot have a one-off form but should have a regular character instead. An audit in the area of information security or an analysis of incidents breaching information security in an organization may provide a starting point for the identification of training needs. Employees themselves may also flag up the need to undergo training in terms of information security (Figure 8).

References

Ahmad, A.; & Maynard, S.B.; & Park, S. 2012. Information security strategies: Towards an organizational multi-strategy perspective, *Journal of Intelligent Manufacturing*, 25(2), 357–370. https://link.springer.com/article/10.1007/s10845-012-0683-0

Albrechsten, E.; & Hovden, J. 2010. Improving information security awareness & behavior through dialogue, participation, & collective reflection. An intervention study, *Journal of Computer & Security*, 29(4), 432-445.

Al--Hamdani, W.A. 2006. Assessment of Need & Method of Delivery for Information Security Awareness Program, *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development (InfoSecCD)*, USA, Georgia, Kennesaw, pp. 102–108.

Balcerek, B.; &Frankowski, G.; & Kwiecień, A.; &, Smutnicki, A.; & Teodorczyk, M. 2012, Security best practices: Applying defense-in-depth strategy to protect the NGI_PL, in *Building a National Distributed e-Infrastructure–PL-Grid* (pp. 128–141), Springer Berlin Heidelberg.

Banerjee, C.; & P&ey, S. K. 2010. Research on software security awareness, *ACM SIGSOFT Software Engineering Notes*, 35(5), 1–5.

Banerjee, C.; & Banerjee, A.; & Murarka, P. D. 2013. An Improvised Software Security Awareness Model, *International Journal of Information, Communication & Computing Technology*, 1(2), 43–48.

Ceglarek, D. 2015, Procedury i narzędzia informatyczne służące do ochrony własności intelektualnej organizacji opartej na wiedzy (IT procedures & tools designed to protect knwoledge-based intellectual property of organizations), *Acta Uniwversitatis Nicolai Copernicus, Zarządzanie* XLII – no. 2,p. 143 https://apcz.umk.pl/czasopisma//index.php/AUNC_ZARZ/article/viewFile/AUNC_ZARZ.2015.024/7322

Chehabeddine, M., Tvaronavičienė, M. 2020. Securing regional development. *Insights into Regional Development*, 2(1), 430-442. http://doi.org/10.9770/IRD.2020.2.1(3)

Chen, C. C.; & Shaw, R. S.; & Yang, S. C. 2006. Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system, *Information Technology Learning & Performance Journal (Organizational Systems Research Association)*, 24(1), 1–14.

Chmura, J. 2017. Forming the awareness of employees in the field of information security, *Journal of positive management*, 8(1), 78–85. https://pdfs.semanticscholar.org/e0fa/550e6826cc70d794d4d2231684f7a0d4e831.pdf

Desman, M. B. 2013. *Building an information security awareness program*. CRC Press.

ENISA 2006. *A users' guide: How to raise information security awareness 2006*. European Network & Information Security Agency, from http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_a_users_guide_how_to_raise_IS_awareness.pdf

ENISA 2007. *Information security awareness initiatives: Current practice & the measurement of success*, from http://www.enisa.europa.eu/act/ar/deliverables/2007/kpistudy/en

EY 2017. Path to cyber resilience: EY's 19th Global Information Security Survey 2016-2017 from http://www.ey.com/Publication/vwLUAssets/ey-globalinformation-security-survey-2016-pdf/$FILE/GISS_2016_Report_Final.pdf

Hadlington, L. 2017. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, & risky cybersecurity behaviours, *Heliyon*, 3(7), 1–18. https://doi.org/10.1016/j.heliyon.2017e00346

Häußinger, F. 2015. *Studies on Employees' Information Security Awareness*; Georg August Universitat Gottingen.

Hellqvist, F.; & Ibrahim, S.; & Jatko, R.; &Ersson, A;. & Hedström, K. 2013. Getting their H&s Stuck in the Cookie Jar – Students' Security Awareness in 1:1 Laptop Schools, *International Journal of Public Information Systems*, 2013(1), 1–19.

ISF. 2002. Effective security awareness (workshop report). *Information Security Forum*, April 2002.

ISF. 2007. *The St&ard of Good Practice for Information Security. Information Security Forum*, available at: https://www.securityforum.org/userfiles/public/2007_sogp_pub.pdf (accessed 23 February 2019).

IT Governance Institute 2007. *IT governance using cobit & val IT (student book, second edtion),* fom http://www.isaca.org/Knowledge-Center/Academia/Documents/Educational

Jabłoński M.; & Mielus M. 2010. Zagrożenia bezpieczeństwa informacji w organizacji gospodarczej (Threats to information security in business organization), in Kwieciński, M. (Ed). *Bezpieczeństwo informacji i biznesu Zagadnienia wybrane*. Oficyna Wydawnicza AFM, Kraków, 23-38

Khan, B.; & Nabi, K.S.; & Khan, M.K. 2011. Effectiveness of information security awareness methods based on psychological theories, *African Journal of Business Management* 5(26), 10862-10868. https://academicjournals.org/articles/search?q=Effectiveness+of+information+security+awareness+methods

Kopijer, P. 2011, *Kompendium zarządzania szkoleniami. Praktyczny przewodnik po inwestycjach w rentowność kapitału kompetencyjnego (Compendium of Training Management. A practical guide to investment in competence capital profitability)*, Wydawnictwo SWPS Academica, Warszawa.

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

Lim, J. S.; & Ahmad, A.; & Maynard, S. 2010. Embedding Information Security Culture Emerging Concerns & Challenges, *Proceedings of the 15th Pacific Asia Conference on Information Systems (PACIS)*, Australia, Brisbane.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., Pattinson, M. (2017), Individual differences & Information Security Awareness, *Computers in Human Behavior*, 69, 151–156. https://doi.org/10.1016/j.chb.2016.11.065

Okenyi, P.O.; & Owens, T. J. 2007. On the Anatomy of Human Hacking, *Information Systems Security*, 16(6), 302–314.

PCI Data Security Standard 2014. *Information Supplement: Best Practices for Implementing a Security Awareness Program*, Security Awareness Program Special Interest Group PCI Security St&ards Council, from https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf?agreement=true&time=1571397048300

Peltier, T.R. 2013. *Information security policies, procedures, & st&ards: Guidelines for effective information security management*. CRC Press.

PN-EN ISO/IEC 27001: 2017-06 System zarządzania bezpieczeństwem informacji.

PWC, 2015. The Global State of Information Security® Survey, https://www.idg.com/tools-for-marketers/global-state-of-information-security-survey-2015/

Rastogi, R. & von Solms, R. (2012). Information Security Service Branding – Beyond Information Security Awareness, *Systemics, Cybernetics & Infomatics*, 10(6), 54–59. https://www.iiisci.org/journal

Rotvold, G.M.; & Braathen, S.J. 2008. Integrating Security Awareness Into Business & Information Systems Education, *Journal of Business & Training Education*, 17, 8–15.

Schultz, E. 2004. Security Training & Awareness---Fitting a Square Peg in a Round Hole. *Computers & Security*, 23(1), 1-2

Shaw, R. S.; & Chen, C. C.; & Harris, A. L.; & Huang, H.-J. 2009. The impact of information richness on information security awareness training effectiveness, *Computers &. Education*, 52(1), 92–100, https://www.sciencedirect.com/science/article/pii/S0360131508001012

Tsohou, A.; & Karyda, M.; & Kokolakis, S.; & Kiountouzis, E. 2015. Managing the introduction of information security awareness programmes in organizations, *European Journal of Information Systems*, 24(1), 38–58.

Vroom, C.; & Von Solms, R. (2004). Towards information security behavioural compliance, *Computers & Security*, 23(3), 191–198, https://www.sciencedirect.com/science/article/pii/S016740480400032X

Tomasz STEFANIUK is the Assistance Professor of Siedlce University of Natural Sciences and Humanities, Specialist of information and communication systems security and ISO 27001 Lead Auditor. Research interests: information security management, management in a virtual environment, design and implementation of communication and information systems.
ORCID ID: orcid.org/ 0000-0001-5769-8735