

Security Awareness from Generation Y Perspective

Gerda Bak

Óbuda University, Doctoral School for Safety and Security Sciences,
bak.gerda@uni-obuda.hu

Anikó Kelemen-Erdős

Óbuda University, Keleti Károly Faculty of Business and Management,
kelemen.aniko@kgk.uni-obuda.hu

Abstract: The sudden and forced digital switchover in the wake of the pandemic has created many situations for which we were not yet prepared. Businesses and educational institutions switched to online solutions overnight but failed to anticipate the problems that this would cause, such as cyber-attacks, when a significant number of these attacks could have been prevented.

In this present research, we used semi-structured in-depth interviews to explore responses to research questions on how Generation Y perceive information security, their awareness of information security and the importance they attach to protecting themselves and their data. The results show that they see their online and digital security as a significant factor. However, in practice, the picture is more different, especially, in terms of appropriate protection methods and their vulnerability. All the interviewees consider themselves as a negligible potential target, even though they are aware that anyone can become a victim. It follows that the security awareness of the respondents need to be improved.

Keywords: cyber security, cyber defence, security awareness, Generation Y, in-depth interview, content analysis

1 Introduction

From online shopping to employment and pleasure, information and communication technology (ICT) has altered and facilitated everyday living [1]. ICT has opened up endless commercial prospects while also posing new problems. Dramatic changes in organisational structures, data management systems, diverse technology ramifications, and information security issues are among the challenges. Information security management has hitherto been handled as a technical issue [2], with much of the focus on technology solutions, but these have proven insufficient. Information security issues should be considered in a management framework, according to several studies [3, 4]. Data security breaches, identity theft, and other internet scams may be catastrophic for businesses, therefore tackling information security is critical.

2 Literature Review

Technology alone cannot provide a reliable solution to organisational information security needs and challenges [2, 5]. Although considerable human-related information security threats remain a major issue, organisations have invested in and continue to invest in technology-based information security solutions (such as firewalls, antivirus software, and intrusion detection systems) to protect their assets [6]. Information security is a persistent challenge at both the corporate and individual levels [7], and to overcome it requires a balanced approach of technological, human and organisational factors [1, 8].

For this reason, it is essential to explore the issue of information security awareness in more detail, of which there are many examples in the literature [9], and a number of factors affecting information security awareness have been studied and identified by researchers, thus studying how to measure [10], develop [11] and predict security awareness. The present research seeks to gain a deeper understanding of the influencing factors and to explore the attitudes of individuals in the aforementioned area. In the related literature, researchers have identified a number of factors that may predict good/appropriate cybersecurity behaviour in the workplace, such as; office environment [12], cybersecurity culture [13], resilience and work stress [14], cognitive skills [15], learning styles [16], personality [17], but also information security experiences play a major role [18].

As can be seen, several factors can influence the security awareness of individuals, but there are also many ways for malicious actors to circumvent these factors. Currently, social engineering attacks are the biggest threat to cyber security [19, 20]. According to Libicki [21], they can be detected but not stopped. Social engineers exploit victims to obtain sensitive information that can be used for specific purposes or sold on the black market and the dark web. With the emergence of Big Data, attackers are using data to monetise valuable data [22]. Huge amounts of data are collected and sold in bulk as commodities in markets [23]. Although social engineering attacks are different, they share a common pattern with similar phases [24].

Organizational information security needs and issues cannot be solved solely through technology [2]. At both the business and individual levels, information security is a constant challenge that requires a balanced strategy of technological, human, and organisational variables to overcome [1].

3 Research Methods

A qualitative approach was used to answer the research questions formulated in the study. This was necessary because qualitative methodology allows us to approach the problem from a perspective that is not possible in quantitative research, thus enabling a deeper analysis [25]. As a tool for this study, we conducted semi-structured in-depth interviews to gain a deeper insight into the

respondents' awareness of information security and their perceptions and opinions about it.

Our main research questions were:

RQ1: How information security is perceived by the individuals?

RQ2: How do respondents perceive the threat posed by digital devices?

During a semi-structured interview, the interviewer follows a guideline and goes through the questions with the interviewees, thus ensuring the comparability of the interviews, and the semi-structured nature of the interview allows the interviewees to express themselves more freely than in a structured interview. This means that the pre-designed questions follow a predetermined sequence [26], and also gives researchers more freedom, as spontaneous questions may arise during the interview [27]. This approach also facilitates a deeper exploration of a more important issue [28].

An argument in favour of the interview is that answering the research questions formulated as research objectives requires deeper and more detailed answers than can be asked or answered in the questionnaire [29]. In addition we approach security awareness in a different way than the one presented above. Content analysis of the interviews was carried out. Data of a quantitative nature, such as word frequency were also analysed and illustrated with a word cloud.

After the semi-structured interviews the interviewees were asked to associate with information security and threats using projective techniques (word association, sentence completion). The essence of word association lies in the fact that, in response to the uttered stimulus words, the respondent is asked to utter the word or idea that first comes to their mind [30]. In the case of sentence completion, since it involves open-ended sentences that the interviewees are asked to complete at their discretion, thus, there are unlimited and varied options in terms of the responses received [31]. The reason for using the two techniques mentioned above was to understand deeper the conducted topic. These techniques are very suitable for this purpose, since with projective techniques, respondents do not have any clue what is the socially expected 'correct' answer to a given word or phrase, unlike in a questionnaire [32].

3.1 Sample

We used only one screening criterion for the potential respondents invited for interviews, in an attempt to reach a potentially wider audience and to get a more detailed picture of the phenomenon under research. As a consequence, the interviewees can be defined by the following parameters: Generation Y, i.e. people born between 1980 and 1994 [33], students and employees, and no restrictions were imposed in terms of education or technological background.

During the interviews, six people were interviewed, three women and three men, among them three students and three employees in terms of occupation. The

youngest interviewee was 27 years old and the oldest 36 years old. The duration of the interviews ranged between 1 and 1.5 hours, and given the pandemic situation, all interviews were conducted online.

4 Results

4.1 Security Awareness

The first research question asked how respondents perceive information security. The interviewees' responses suggest that they associate information security with data protection and control over information sharing, as well as information self-determination. In terms of importance, the interviewees consider information security to be an important factor, which is useful as well as necessary. In contrast, there were two opinions that there is no doubt that we need to pay attention to the protection of our data and smart devices, but this is not easy, as it is '*sometimes overcomplicated*'. This points to the complexity of the perception of security.

4.2 Association about Information Security

As mentioned earlier in this paper, word association and sentence completion techniques were used in the final stage of the interviews. In the case of word association, the respondents made associations about six phrases, while in the case of sentence completion, the supplements of four phrases were applied.

Figure 1. illustrates the different associations about the diverse factors of information security. The word 'spam' evoked their negative thoughts, mass-mailing, and filtering solution. The second stimulus was the term 'virus killer', about which respondents thought of as a specific antivirus program, or as a basic tool for protection. The next in line was 'cyber defence'. There were fewer identical or unanimous answers. Some of the respondents associated it with attack and perpetrators, while the other interviewees approached it from a relatively positive or neutral perspective, such as a means of defence and its role in defence. The fourth pendulum that was raised was 'data theft'. Again, the responses were mainly negative, such as 'trouble, it can happen to anyone' (I1), but there were also some who responded by monitoring and detecting data theft, or more specifically by mentioning a software tool (Wireshark) that is able to explore these kind of problems. The penultimate word 'security settings' elicited mixed and even conflicting opinions from the interviewees. On the one hand, it was referred to as a fundamental factor, but on the other hand, it was also perceived as a complex term, requiring greater expertise. Finally, the perceptions of cyber-attacks were explored. Here again, negative feelings and reactions to it dominated, such as 'never' (I3) or 'danger' (I4).

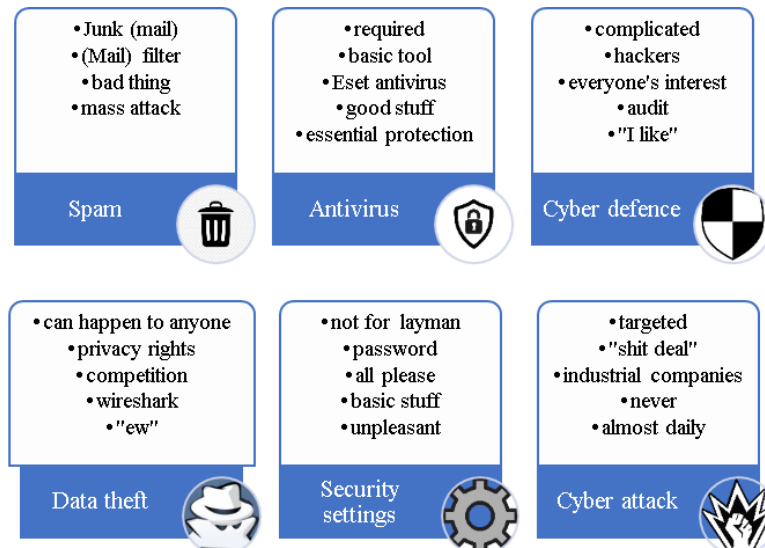


Figure 1 Word associations about different factors of information security

4.3 Assosiations about Security Awareness and Cyber Attacks

The associations obtained in the sentence completions are shown in Figure 2. Responses that may have been given by more than one person are shown only once, and the number of similar/same responses is shown in parentheses after each response.

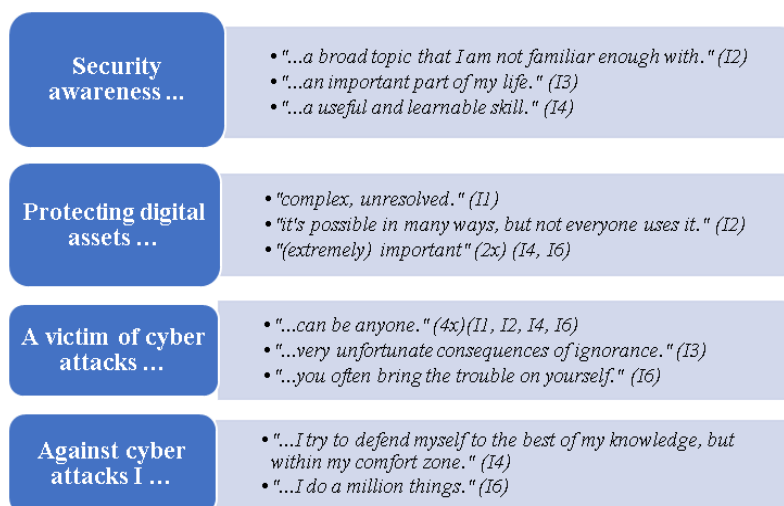


Figure 2 Associations about cyber security and attacks

An example of the multiple occurrences mentioned above is in this case the responses to the fourth sentence, where two subjects added that the victim of cyber-attacks is often the victim of their own fault or ignorance, or the consequence of these, while four interviewees said that the victim of cyber-attacks could be anyone. Figure 2 shows the most focused answers that interviewees responded to in the sentence completion. The respondents were unanimously positive about security awareness. Similar to previous results, they consider it a learnable or essential factor.

The picture is more nuanced when it comes to the protection of their digital devices, which is also considered to be an important issue in their lives, but there are also some responses that suggest that they have problems with it. Such responses include that the digital devices are 'complicated' (I4), 'too complex' (I1), or even 'almost impossible to achieve' (I3). The responses on victims of cyber-attacks were similar to the interview responses, i.e. on the one hand, anyone can be a victim, and on the other hand, the victim becomes a victim through no fault of his/her own. Apart from these answers, there is a certain level of safety awareness on the part of the interviewees, which is somewhat questioned by the answers to the next and last sentence to be added.

The answers suggest that the interviewees are trying to do something about cyber attacks, but most of them are not doing as much as they should. This is supported by the responses indicating that these interviewees are making limited efforts, as long as they are 'within their comfort zone' (I4).

Conclusions

The aim of this research was to provide a picture of Generation Y users' information security awareness, associations and attitudes towards cybersecurity and cyber-attacks. Although the qualitative nature of this research means that it is not representative, does not allow for generalisation, and broad conclusions to be drawn from the results, this can provide useful insights as a baseline study. Further research, including in-depth interviews with business leaders, would help to provide a different perspective.

The level of security awareness of interviewees is inadequate, sometimes far below their knowledge and understanding of information security. This is in line with several international studies [34, 35]. According to some research, if the user is not aware of an attack, does not recognise the signs of a potential attack, then knowledge of the threats and the means to protect against them are futile [36]. Another research suggests that knowledge of the underlying motives behind the rules protecting the user and the user's understanding of the logical relationships contribute to more security-aware behaviour [37].

A novel finding related to the foregoing is that subjects underestimate their own vulnerability. Despite the fact that, according to their own account, anyone can be a victim of social engineering, the interviewees feel that they are not targeted for

various reasons (job, income, online activity, etc.). International research shows that if someone misjudges their own risk exposure, they are more likely to engage in more risk-taking activities in the online space [38].

As the results show and suggest, there is a need to prioritise security awareness at both individual and organisational level in the near and distant future. Furthermore, it is worth reflecting on the reasons for the existence of a gap between knowledge and awareness and ways to reduce it.

Acknowledgement

Supported by the ÚNKP-21-3 New National Excellence Program of the Ministry for Innovation and Technology from the Source of the National Research, Development and Innovation Fund.

References

- [1] Soomro, Z.A., Shah, M.H., Ahmed, J.: Information security management needs more holistic approach: A literature review, *International Journal of Information Management*, 2016, 36, (2), pp. 215-225
- [2] Singh, A.N., Picot, A., Kranz, J., Gupta, M.P., Ojha, A.: Information Security Management (ISM) Practices: Lessons from Select Cases from India and Germany, *Global Journal of Flexible Systems Management*, 2013, 14, (4), pp. 225-239
- [3] Hu, Q., Dinev, T., Hart, P., Cooke, D.: Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*, *Decision Sciences*, 2012, 43, (4), pp. 615-660
- [4] Cram, W.A., Proudfoot, J.G., D'Arcy, J.: Organizational information security policies: a review and research framework, *European Journal of Information Systems*, 2018, 26, (6), pp. 605-641
- [5] Tick, A., Kárpáti-Daróczy, J., Saáry, R.: To familiarise or not to familiarise' - industry 4.0 implementation in SMEs in Hungary, in Trumić, M. (Ed.): 'Possibilities and barriers for Industry 4.0 implementation in SMEs in V4 countries and Serbia' Atlantis, 2022, pp. 35-61
- [6] Abawajy, J.: User preference of cyber security awareness delivery methods, *Behaviour & Information Technology*, 2012, 33, (3), pp. 237-248
- [7] Mai, P.T., Tick, A.: Cyber Security Awareness and Behavior of Youth in Smartphone Usage: A Comparative Study between University Students in Hungary and Vietnam, *Acta Polytechnica Hungarica*, 2021, 18, (8), pp. 67-89
- [8] Saáry, R.: A vállalati biztonság a stakeholder elmélet tükrében. PhD disszertáció, Óbudai Egyetem, 2021
- [9] Ahlan, A.R., Lubis, M., Lubis, A.R.: Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures, *Procedia Computer Science*, 2015, 72, pp. 361-373
- [10] Al-Alawi, A.I., Al-Kandari, S.M.H., Abdel-Razek, R.H.: Evaluation of Information Systems Security Awareness in Higher Education: An Empirical Study of Kuwait University, *Journal of Innovation and Business Best Practice*, 2016, 2016, pp. 1-24

- [11] Zhongping, Z., Kaifeng, Y., yi, Z., Peipei, Z.: Increasing Employees' Awareness and Enhancing Motivation in E-Government Security Behavior Management: '2013 Fourth International Conference on Digital Manufacturing & Automation' IEEE, 2013, pp. 684-687
- [12] Pattinson, M., Ciccarello, B., Butavicius, M., Parsons, K., McCormac, A., Calic, D.: Is your office environment conducive to good cyber security behaviour?: 'Proceedings of the 17th Australian Cyber Warfare Conference (CWAR), Melbourne, Australia', 2018, pp. 32-41
- [13] Wiley, A., McCormac, A., Calic, D.: More than the individual: Examining the relationship between culture and Information Security Awareness, *Computers & Security*, 2020, 88, pp. 101640
- [14] McCormac, A., Calic, D., Parsons, K., Butavicius, M., Pattinson, M., Lillie, M.: The effect of resilience and job stress on information security awareness, *Information & Computer Security*, 2018, 26, (3), pp. 277-289
- [15] Jaeger, L.: Information Security Awareness: Literature Review and Integrative Framework: 'Proceedings of the 51st Hawaii International Conference on System Sciences' HICSS, 2018, pp. 4703-4712
- [16] Pattinson, M., Butavicius, M., Lillie, M., Ciccarello, B., Parsons, K., Calic, D., McCormac, A.: Matching training to individual learning styles improves information security awareness, *Information & Computer Security*, 2019, 28, (1), pp. 1-14
- [17] Azucar, D., Marengo, D., Settanni, M.: Predicting the Big 5 personality traits from digital footprints on social media: A meta-analysis, *Personality and Individual Differences*, 2018, 124, pp. 150-159
- [18] Albrechtsen, E.: A qualitative study of users' view on information security, *Computers & Security*, 2007, 26, (4), pp. 276-289
- [19] Chargo, M.A.: You've Been Hacked: How to Better Incentivize Corporations to Protect Consumers' Data, Transactions: The Tennessee Journal of Business Law, 2018, 20, pp. 115-143
- [20] Costantino, G., La Marra, A., Martinelli, F., Matteucci, I.: CANDY: A Social Engineering Attack to Leak Information from Infotainment System: '2018 IEEE 87th Vehicular Technology Conference (VTC Spring)' IEEE, 2018, pp. 1-5
- [21] Libicki, M.: Could the Issue of DPRK Hacking Benefit from Benign Neglect?, *Georgetown Journal of International Affairs*, 2018, 19, (1), pp. 83-89
- [22] Atwell, C., Blasi, T., Hayajneh, T.: Reverse TCP and Social Engineering Attacks in the Era of Big Data: '2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)' IEEE, 2016, pp. 90-95
- [23] Mahmood, T., Afzal, U.: Security Analytics: Big Data Analytics for cybersecurity: A review of trends, techniques and tools: '2013 2nd National Conference on Information Assurance (NCIA)' IEEE, 2013, pp. 129-134
- [24] Mouton, F., Leenen, L., Venter, H.S.: Social engineering attack examples, templates and scenarios, *Computers & Security*, 2016, 59, pp. 186-209
- [25] Kelemen-Erdős, A.: Dead-end development or real progress? Paradigm shift initiatives in marketing theory, in Živan, Ž. (Ed.): 'An international serial

publication for theory and practice of Management Science: IMCSM Proceedings' University of Belgrade, 2019, pp. 26-38

[26] Molnár, D.: Empirikus kutatási módszerek a szervezetfejlesztésben, Humán Innovációs Szemle, 2010, 1, (1-2), pp. 61-72

[27] Hove, S.E., Anda, B.: Experiences from Conducting Semi-structured Interviews in Empirical Software Engineering Research: '11th IEEE International Software Metrics Symposium (METRICS 2005)' IEEE, 2005, pp. 23-23

[28] Kelemen-Erdős, A., Mitev, A.Z.: Eszképizmustól az ajánlásig – Élményfokozatok és hatásai a romkocsmákban, Turizmus Bulletin, 2020, 20, (2), pp. 14-21

[29] Malhotra, N.K., Simon, J.: Marketingkutatás. Budapest: Akadémiai Kiadó, 2017

[30] Aiken, L.R., Groth-Marnat, G.: Psychological Testing and Assessment. Boston: Allyn and Bacon, 2006, 12th edn

[31] Horváth, D., Mitev, A.: Alternatív kvalitatív kutatási kézikönyv. Budapest: Alinea Kiadó, 2015

[32] Steinman, R.B.: Projective Techniques in Consumer Research, International Bulletin of Business Administration, 2009, 5, (1), pp. 37-45

[33] Tari, A.: Y generáció - Klinikai pszichológiai jelenségek és társadalomlélektani összefüggések az információs korban. Budapest: Jaffa Kiadó és Kereskedelmi Kft., 2010

[34] Alzubaidi, A.: Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia, Heliyon, 2021, 7, (1), pp. e06016

[35] Butavicius, M., Parsons, K., Lillie, M., McCormac, A., Pattinson, M., Calic, D.: When believing in technology leads to poor cyber security: Development of a trust in technical controls scale, Computers & Security, 2020, 98, pp. 102020

[36] Bolat, P., Kayışoğlu, G.: Antecedents and Consequences of Cybersecurity Awareness: A Case Study for Turkish Maritime Sector, Journal of ETA Maritime Science, 2019, 7, (4), pp. 344-360

[37] Ngoqo, B., Flowerday, S.V.: Information Security Behaviour Profiling Framework (ISBPF) for student mobile phone users, Computers & Security, 2015, 53, pp. 132-142

[38] Beldad, A.D.: Sharing to be sociable, posting to be popular: factors influencing non-static personal information disclosure on Facebook among young Dutch users, International Journal of Web Based Communities, 2015, 11, (3/4), pp. 357