

Information security awareness vs cyber security awareness vs internet safety awareness

Gerda Bak

Óbuda University,
bak.gerda@uni-obuda.hu

Jolán Velencei

Óbuda University,
velencei.jolan@kgk.uni-obuda.hu

Abstract: One of the great challenges of the 21st century is digitalisation, which has brought with it the emergence of Industry 4.0 and the high connectivity of smart devices. This accelerated development has significantly transformed the way individuals live and think, as well as their vulnerability.

In the literature on the relationship between digital devices and individuals, there are significant differences in the way individuals' security is threatened and the factors and behaviours that facilitate and enhance their security. The COVID-19 pandemic and its aftermath, which has dominated the last 2-3 years, only adds to the importance of this area of study.

The aim of the present research is to examine the differences and similarities between publications on information security awareness, cyber security awareness and internet safety awareness and to summarise their results, for which a literature review was conducted.

Keywords: *information security awareness, cyber security awareness, internet safety awareness, literature review*

1 Introduction

In the last 5-10 years, we have seen a rapid development of technology, which Covid has only added to [1]. The information and communications technology (ICT) is inescapable part of our lives [2]. The rise of smartphones, smart working and the home office. The problem is more that technology is developing at a faster pace than we are [3]. The pandemic is a good example of the fact that we are, so to speak, just following and adapting to the achievements of digitalisation [4]. Looking at the research, studies and articles on digital tools, information security and the online space, there is no uniform and agreed approach either in the definitions or in the labelling [5, 6]. In the formulation of Von Solms and Van Niekerk [7], information security and cybersecurity overlap to some extent. In a later study, they defined cybersecurity as part of information security [8].

That is why the question arises: do we even know the basics, do we know the phenomena and the definitions? The research are based on the fact that these three concepts are interchangeable in the minds of many people [7], and that there are many different definitions [9] because of the many research aspects of the topic and the transdisciplinary nature of the subject [10, 11].

The structure of the paper is as follows. The Section Two presents the conceptual background and state of the topic. Section Three presents the research methodology. The findings are reported in Section Four. The research's theoretical and applied contributions are provided in Section Five.

2 Literature Review

In defining awareness, there are a number of factors that make it difficult to arrive at a single definition. Some definitions of awareness also contain procedural features, i.e., the procedures employed to create this state of mind, in addition to aspects of an individual's cognitive state of mind, such as being conscious or knowing something [12-14]. There are not many definitions that separate awareness from a certain type of activity [15].

Although security and privacy play a prominent role in research on information systems [16], research on the human aspect, such as the managerial approach to information security [2, 17], information security awareness [17, 18] and the role of human factors and CEOs [19, 20] have only become the focus of academic studies in the last few years.

The term cybersecurity is often used interchangeably with information security, and although there is a significant overlap between cybersecurity and information security, the two concepts are not fully compatible [7]. Cybersecurity and internet security are like two sides of the same coin. However, other professionals think that cyber-security is a division or subfield of internet safety [21].

Some studies have argued that cybersecurity goes beyond traditional information security and encompasses the protection not only of information resources but also of other assets, including the person. The reference to the human factor in information security generally refers to the role of the human in the security process. In the case of cybersecurity, the human being is perceived as a potential target of cyber-attacks, or even unwittingly becomes a party to a cyber-attack. This additional dimension has ethical implications for society as a whole, as the protection of certain vulnerable groups, e.g. children, can be seen as a social responsibility [7].

In order to understand the concepts we have just discussed, we need to know the basic phenomena that go with them.

- Information Security protects all forms of data from unauthorized access, modification, deletion, etc. It secures data from all types of attacks.

- Cyber Security on the other hand, protects digital data from external threats like trojans, viruses, hackers, and other malicious activities that can take place on the internet. It mainly protects data available in cyberspace from various cyber threats [8].
- Online safety refers to the act of staying safe online. It encompasses all technological devices which have access to the internet from PCs and laptops to smartphones and tablets. Being safe online means individuals are protecting themselves and others from online harms and risks [22].

3 Research Methods

This publication sought to synthesise the body of knowledge in this field. Two key sections make up this study. The quality of any review article is greatly influenced by the literature search that takes up the majority of the first section. A thorough, systematic search technique has been used to find pertinent material for this. Analysis and synthesis of the identified literature make up the second section. To this a systematic literature review was used. Before producing a review, the literature review process involves four stages: planning, selection, extraction, and execution [23].

In the research using one large digital library, ScienceDirect. International journal publications between 2010 and 2020 were examined. The reviews, proceedings, book chapters were excluded. Papers in other languages than English were excluded as well. The inclusion and exclusion criteria are determined by and used in the selection of the article. The inclusion and exclusion criteria listed in Table 1.

The next keywords were used in the search are: “Information security awareness”, “Cyber security awareness”, “Internet safety awareness”. This resulted in 192 studies in the first round.

Inclusion criteria	• written in English, • published between 2010 and 2020
Exclusion criteria	• studies from organization report, opinion papers, and editorial, not research article, • measure security awareness, • examine what factors influencing the security awareness, • does not apply to the individual, • not relevant, out of scope, • tries to solve with technology • developed a measurement tool, or a framework • looked at the tasks of managers/CISO

Table 1 Criteria inclusion and exclusion

The relevant papers were selected in more rounds, based on different criteria, identified to ensure relevance and rigour. A first round of filtering focused on technical aspects: results were narrowed down by including only journal articles, as representative of methodological rigour [24]; documents in other languages than English were excluded; and so were duplicates across databases. A second

round of filtering focused on metadata aspects: false positives were excluded where, for example, the terms “information security awareness” helyett just “information security” were found. A third round of filtering focused on substantial aspects: extensive analysis of abstracts led to the exclusion of documents that were out of scope (e.g., the problem of information security management was solved by technical ways; research focus was only on university students, or examined individuals' online behaviours; or analysed the ISO standards). After this refinement, a total of 55 paper were analysed deeper. To stay on topic, a systematic literature review needs clear research questions. Table 2 presents the research questions for this literature review.

	Research questions	Research aim
RQ1	How do some researchers interpret Information security awareness, Cyber security awareness and Internet safety awareness?	Identify the similarities and differences between each concept.
RQ2	How can organisations raise the information security awareness of their employees?	Identify suggestions and solutions for raising awareness in the area of information security

Table 2. Research question for the literature review.

3.1 Areas of analysis

The definition of the three phenomena we are looking for, their context, or who they were investigated on, and the study findings are the four areas of analysis on which we have concentrated. This refers to the advantages of increasing awareness and the methods for doing so that have been established.

Definitions	Information security awareness Cyber security awareness Internet safety awareness
Context	Target groups
Techniques for raising awareness	Main solutions used to support target groups in achieving compliance with cyber security and security-related behaviours
Benefits of awareness	Benefits resulting from improving awareness

Table 3 Aspects considered

4 Results

4.1 Applied Research methods and the target groups

We also looked at the research methods used by each researcher on the topic. We did not find any really big differences in this area, as most of the publications use questionnaires, interviews or literature research similar to ours. In details it can be seen in the Table 4 below.

Topic	Research method	Target group
Information security awareness	• literature review, • questionnaire, • interviews/ case studies, • experiment, • modelling/simulations	• Students, • teachers • employees, • managers, professionals
Cyber security awareness	• literature review, • questionnaire, • interviews/ case studies, • experiment	• students, • professionals • users
Internet safety awareness	• questionnaire • interviews	• students • teachers • parents

Table 4 Summarized of the research methdes and target groups by awareness

4.2 Definitions of the three awareness

The 55 studies included in the in-depth analysis were also examined in terms of how the authors of the study defined the awareness in question (information, cyber or internet). Most of the studies examined did not discuss definitions, but only highlighted the importance of the topic in general terms, possibly in the direction of statistical data. However, those studies that did include some definition of the awareness in question were selected and compared with each other. The results of this comparison are presented in Table 5 below.

Term	Definition
Information security awareness	Understanding of information security policies, rules, and responsibilities, as well as security risks and the effects they have.
Cyber security awareness	The amount of users' awareness of information security's significance and their obligations to exert adequate degrees of information control to safeguard networks and data.
Internet safety awareness	Users must have the skills necessary to properly manage their online activities, understand how to handle uncomfortable and inappropriate information, and know when to ask for assistance.

Table 5 Summarized of the definitions

The table clearly shows that while information security awareness and cyber security awareness are conceptualised by many as a certain kind of knowledge and understanding, internet security awareness involves a skill in addition to knowledge.

• 4.1.2 Techniques for raising awareness and the benefits

When it comes to increasing safety awareness, researchers have tried and identified a relatively wide range of potential tools and methods to increase an individual's safety awareness. Most of the techniques identified are related to information security awareness, the reason being that in terms of number of publications, there were more publications in the database we used to identify this term. The summary results are presented in Table 5 below.

Term	Techniques	Benefits
Information security awareness	- developing, improving security culture - implementing a security policy - Information safety awareness programs, frameworks - workshop, training - promoting a safety culture - information security knowledge sharing, collaboration - involving IT management and employees in security precautions and policy development	- reduce the risk of employee misbehaviour and harmful interaction with information assets - improve perceptions of IS risk, responsibilities, ISP importance, and knowledge - attitude towards compliance with organizational information security policies - improve the knowledge of users' information security - IT managers can be more engaged and motivated in planning and executing IS awareness programmes
Cyber security awareness	- cyber security awareness program - education, conference, training - gamification, table and cardgames - management support in cyber security issues and related concerns - involving IT management and employees in security precautions and policy development	- avoid security incident - increase users' cyber hygiene behaviors or knowledge - players of the game can get an understanding of security attacks and vulnerabilities - preventing cyber security threats - employees can have an understanding of the limitations of cyber security technical safeguards
Internet safety awareness	- training - promoting a safety culture - parental mediation	- decrease incidents - employees have a positive attitude - greater commitment to security

Table 5 Techniques to increase security awareness and their potential benefits in the studies reviewed

It can be considered as a progressive and positive observation that there is also an emergence of research that seeks to assess the results that can be achieved through gamification in an unconventional way, as well as through tools that require the active involvement of participants, and that is considered as a viable way forward in comparison to training and education.

Conclusions

With the rapid spread of digital technologies and the services they provide, users are enjoying a range of benefits that greatly enhance their convenience and simplify their lives. But it also exposes them to a number of risks. With increasing exposure to threats and potential risks, digital and cybersecurity knowledge and skills have become a vital skill for all cyber citizens. Therefore, as important and necessary skills, they need to be integrated into the everyday cyber behaviour of individuals to the extent that it becomes an unconscious action, i.e. not only increasing their knowledge and awareness on the subject, but also their awareness.

Access to the internet and the use of ICT tools present a number of risks, which can have serious consequences for users with limited or no information security knowledge. These users are therefore exposed to serious risks, the reduction of which is in everyone's interest. It is therefore essential to ensure that users are educated, understand security risks, ways of limiting risks and the basic concepts and factors involved

The literature shows that there are many studies on individual awareness [2], whether it is information or cyber security awareness or even internet safety awareness, but there are also suggestions for frameworks and guidelines for promoting information security cultures [25]. Nevertheless, it is worth taking a step back and starting from the basics, since, as this study has pointed out, there are no widely accepted definitions or guidelines on what constitutes awareness, or indeed on the relationship between the two. The present study has sought to bridge this gap and bring it closer to lay people. Although not exhaustive, which could be formulated as a limitation of the research, it highlights questions and ideas that need to be taken into account in the future.

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] Vargo, D., Zhu, L., Benwell, B., Yan, Z.: Digital technology use during COVID -19 pandemic: A rapid review, *Human Behavior and Emerging Technologies*, 2020, 3, (1), pp. 13-24
- [2] 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
- [3] Sima, V., Gheorghe, I.G., Subić, J., Nancu, D.: Influences of the Industry 4.0 Revolution on the Human Capital Development and Consumer Behavior: A Systematic Review, *Sustainability*, 2020, 12, (10), pp. 4035
- [4] Bongiovanni, I.: The least secure places in the universe? A systematic literature review on information security management in higher education, *Computers & Security*, 2019, 86, pp. 350-357
- [5] Reid, R., Van Niekerk, J.: From information security to cyber security cultures: '2014 Information Security for South Africa' IEEE, 2014, pp. 1-7
- [6] de Oliveira Albuquerque, R., García Villalba, L.J., Sandoval Orozco, A.L., de Sousa Júnior, R.T., Kim, T.-H.: Leveraging information security and computational trust for cybersecurity, *The Journal of Supercomputing*, 2015, 72, (10), pp. 3729-3763
- [7] von Solms, R., van Niekerk, J.: From information security to cyber security, *Computers & Security*, 2013, 38, pp. 97-102
- [8] von Solms, B., von Solms, R.: Cybersecurity and information security – what goes where?, *Information & Computer Security*, 2018, 26, (1), pp. 2-9
- [9] 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
- [10] Rajaonah, B.: Une vision de la recherche sur la confiance et la sûreté des systèmes d'information dans le cadre de la protection des infrastructures critiques, *Ingénierie des systèmes d'information*, 2017, 22, (1), pp. 109-133
- [11] Dodig-Crnkovic, G., Kade, D., Wallmyr, M., Holstein, T., Almér, A.: Transdisciplinarity Seen Through Information, Communication, Computation, (Inter-)Action and Cognition, in Burgin, M., and Hofkirchner, W. (Eds.): 'Information Studies and the Quest for Transdisciplinarity - Unity through Diversity' World Scientific, 2017, pp. 217-261
- [12] Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness, *MIS Quarterly*, 2010, 34, (3), pp. 523-548

- [13] D'Arcy, J., Hovav, A., Galletta, D.: User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach, *Information Systems Research*, 2009, 20, (1), pp. 79-98
- [14] Tsohou, A., Karyda, M., Kokolakis, S., Kiountouzis, E.: Managing the introduction of information security awareness programmes in organisations, *European Journal of Information Systems*, 2017, 24, (1), pp. 38-58
- [15] Spears, J., Barki, H.: User Participation in Information Systems Security Risk Management, *MIS Quarterly*, 2010, 34, (3), pp. 503-522
- [16] Lowry, P.B., Dinev, T., Willison, R.: Why security and privacy research lies at the centre of the information systems (IS) artefact: proposing a bold research agenda, *European Journal of Information Systems*, 2018, 26, (6), pp. 546-563
- [17] Siponen, M., Adam Mahmood, M., Pahlila, S.: Employees' adherence to information security policies: An exploratory field study, *Information & Management*, 2014, 51, (2), pp. 217-224
- [18] Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., Zwaans, T.: The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies, *Computers & Security*, 2017, 66, pp. 40-51
- [19] Curry, S.: Boards Should Take Responsibility for Cybersecurity. Here's How to Do It. 2017 Letöltve: 19.05.2022, <https://hbr.org/2017/11/boards-should-take-responsibility-for-cybersecurity-heres-how-to-do-it>
- [20] Jaeger, J.: Human error, not hackers, cause most data breaches, *Compliance Week*, 2013, 10, (110), pp. 56-57
- [21] Chatterjee, R.: Difference Between Cybersecurity & Information Security. 2020 Letöltve: 15.05.2022, <https://analyticsindiamag.com/difference-between-cybersecurity-information-security/>
- [22] Maurer, T., Morgus, R.: Compilation of Existing Cybersecurity and Information Security Related Definitions, in Editor (Ed.)^(Eds.): 'Book Compilation of Existing Cybersecurity and Information Security Related Definitions' New America, 2014, edn., pp.
- [23] Okoli, C., Schabram, K.: A Guide to Conducting a Systematic Literature Review of Information Systems Research, *SSRN Electronic Journal*, 2010, 10, pp. 1-51
- [24] Paré, G., Tate, M., Johnstone, D., Kitsiou, S.: Contextualizing the twin concepts of systematicity and transparency in information systems literature reviews, *European Journal of Information Systems*, 2017, 25, (6), pp. 493-508
- [25] Angraini, Alias, R.A., Okfalisa: Information Security Policy Compliance: Systematic Literature Review, *Procedia Computer Science*, 2019, 161, pp. 1216-1224