Esmeralda Kadena
Óbuda University, Doctoral School on Safety and Security Sciences,
Ph.D. Candidate,
kadena.esmeralda@uni-obuda.hu

Dr. Marsidi Gupi
University College of Business, Rruga Vangjel Noti, Tirana, Albania
Head of Law Department,
mgupi@kub.edu.al

DOI: 10.37458/ssj.2.2.3
Research Paper
Received: October 13, 2021
Accepted: December 10, 2021

HUMAN FACTORS IN CYBERSECURITY: RISKS AND IMPACTS

Abstract: Technological solutions in the mobile and digital era are becoming more helpful in informing the population, educational systems, monitoring, tracking the individuals, working, and spending time from home. On the other hand, the valuable information within such systems is posed to the risk of breaches at the individual and organizational level. As a result, cyber threats are constantly evolving. Many security incidents and data breaches are associated with the human factor. Respectively, this work highlights the importance of human factors in cybersecurity. Firstly, this article gives a brief overview of the topic and its significance. Then we present the most common risks in the cybersecurity field and their impacts. The third part emphasizes the role of human factors in security and elaborates on the behavioral approaches. Our conclusions are drawn in the last detail. To further our research, we plan to investigate behavioral science theories on understanding the influence of human factors in cybersecurity.
Keywords: Cybersecurity, Cyber risks, Human Factor, Impacts.

1. INTRODUCTION

Society is becoming more and more technology-dependent and simultaneously more vulnerable to cybercrime. According to the 2020 Cybercrime Report of Herjavic Group, cybersecurity threats in 2021 were expected to cost the world the US $ 6 trillion a year – twice as in 2015 (Herjavec Group, 2020). A report of the Cybersecurity Insiders pointed out that in 2020 around

68% of organizations felt “moderately to extremely vulnerable” to insider threats (Cybersecurity Insiders, 2020). During the COVID-19 pandemic, health care organizations become the first targets, and the number of cyberattacks has been increased five-fold (World Health Organization, 2020). Similar was the (post) Hurricane Katrina case in 2005, where thousands of new fraudulent websites offered false government support (FBI, 2015).

Critical situations are perfect for cybercriminals because they can take advantage of the weakest link in the security chain - the human factor. Individuals’ fear, carelessness, and lack of awareness and information in such situations make them more susceptible to falling for scams. Cybercriminals use human factors to get unauthorized access, steal credentials, and infect systems with malware. Cyber-attacks are on the rise. They are not as expensive as physical attacks, not limited to distances and geography, and cannot be easily tracked and identified. Thus, these attacks are more attractive and dangerous than the physical ones. In addition, malicious programs can be reused to attack other systems.

Cybersecurity is developing to tackle the range of attack types while the attackers respond with their innovative hacking methods. Cybersecurity uses different approaches to increase detection of the threats, such as multi-factor authentication (MFA), Network Behavioral Analysis (NBA), Threat Intelligence and automatic update, real-time protection, sandboxing, forensics, back-up and mirroring, and Web app firewalls (Shabut, Lwin and Hossain, 2016). Nonetheless, the centralization of massive amounts of user data, personal information, and the availability of data up to date have made social networking an attractive target for organizations that have legitimate purposes as well as malicious ones. Furthermore, with the proliferation of the IoT and the ongoing digitalization of many aspects of life, cybercriminals have more exploiting opportunities (Kadëna and Kerti, 2017). Therefore, security remains a critical issue for individuals and organizations.

2. CYBER RISKS AND IMPACTS

In the literature exist several definitions regarding information security. However, the most dominating report relies on the triad CIA security model mentioned first in a NIST publication (ISO/IEC, 2018) (Neumann, Statland, and Webb, 1977). The triad model is comprised of three elements (Andress, 2011):

- Confidentiality: information should not be available or disclosed to individuals, entities, or processes without authorization. It can be considered equal to privacy.
- Integrity: maintaining the accuracy, completeness, and trustworthiness of data.
- Availability: information and data should be accessible and usable from the authorized entities.

An attack that is successfully realized can compromise this triad. Theft and espionage can result in financial, proprietary, and personal information loss. Risk reduction varies among sectors and organizations. For instance, the level of cybersecurity expected from customers may be lower for a company in the entertainment sector than for a hospital, a bank, or a government agency. To better understand cyber risks and their consequences, we represent a categorization of malware and system vulnerabilities.

2.1. Malware

Nowadays, malware attacks are used mainly to steal personal, business, and financial information that can benefit others (Cluley, 2010), (Schultz, 2006). Typical targets are governments or organizations' websites to disrupt their operations or gather sensitive information. Besides, attackers use this tool to steal the personal information of individuals, such as credit card numbers. Due to the widespread and convenience of Internet access, malware use has been increased for for-profit purposes (Bayer *et al.*, 2009). Cybersecurity experts have been trying to tackle cyber-crime problems. They believe that malware is a crucial tool used for attacks in the cybersecurity field (Australian Parliament. House of Representatives, 2010).
The malware attacks are loaded on a system without the legitimate owner's knowledge and intend to break or compromise the system. The most common forms of malware are viruses, worms, spyware, and bot executables (Cárdenas *et al.*, 2008). There are a variety of ways hackers use to infect systems. They can infect the target machines, manipulate users to open infected files (social engineering methods), or convince them to visit attractive websites. Most of

them have been designed to control targets' computers for black market exploitation like sending spam emails or monitoring users' web browsing behaviors. The most common ways of malware attacks are classified as follows.

2.1.1. Spam

Spam is malware that sends irrelevant, inappropriate, and unrequested messages to a list of recipients. In the second quarter of 2021, corporate accounts have been the most tempting targets for cybercriminals (Kulikova and Shcherbakova, 2021).

2.1.2. Phishing

Phishing refers to attempts to obtain users' credentials or bank account details by impersonating them (Cloudflare, 2020). Cybercriminals have taken advantage of the pandemic, hunted for account credentials, and exploited the COVID-19 theme. They have used links in emails, scammers, and imitated emails from popular cloud services. Most phishing methods use technical deception to create links in emails and spoofed websites that belong to a legitimate organization.

2.1.3. Downloads

A drive-by download is a form attackers use to spread malware fast. There is no regular communication between the target endpoints and company servers. Users can get triggered when they visit a website while viewing an email message or clicking on a deceptive pop-up window. Surveys have shown that an increasing number of web pages have been infected, and various types of malware have been discovered (RSA, 2021). When a user visits the malicious website, malware is downloaded and automatically installed in the victim's machine without his knowledge (Kanich *et al.*, 2008).

2.2. System Vulnerabilities

Once malware is present in the victim's system, cybercriminals can search and utilize aspects of existing vulnerabilities in the system to use them in their malicious activities. The most commonly exploited vulnerabilities are in systems' hardware, software, network infrastructure, and protocol (Jang-Jaccard and Nepal, 2014).

2.2.1. Hardware

Hardware is considered the most manipulative system. If the hardware is compromised, attackers have the flexibility and power to launch security attacks (Li *et al.*, 2008). Because yet there is a lack of tools for detecting hardware attacks, they have been on the rise (Potlapally, 2011). Trojans are the most common hardware exploits. They are malicious and deliberately secretive made to Integrity Circuits in the hardware (Chakraborty, Narasimhan and Bhunia, 2009). For example, a trojan in the system's hardware can cause an error detection module to accept inputs that should not be taken (Kulikova and Shcherbakova, 2021). In addition, it can insert more buffers in the interconnections of the chip resulting in consuming more power that could decrease the battery efficiency quickly. In addition, Denial-of-Service (DoS) Trojans might prevent operating a specific function or resource (Kadena, Nguyen, and Ruiz, 2021). DoS attacks can exhaust systems' bandwidth, computation, and battery power. Moreover, such attacks might physically destroy, disable, or change the configuration of a device. For example, attacks against control systems can cause damage or interruption of machines they control, like centrifuges, generators, and pumps (Kadena, 2018).

2.2.2. Software

Cyber-attacks can use software errors, flaws, or faults in computer programs (internal OS, external interface drivers, applications) to make systems behave differently from their original way (Shahriar and Zulkernine, 2012). These errors, flaws, or faults in the systems are commonly known as bugs. Liu and Cheng found that most attacks have occurred by exploiting software vulnerabilities caused by bugs and design flaws (Liu and Cheng, 2009). In addition, studies have

shown that software vulnerabilities often arise because of software bugs in memory, user input validation, and user access privileges (Tsipenyuk, Chess and McGraw, 2005) (McGraw, 2006). Buffer overflow is a technique cybercriminals use to interfere with existing process code. Buffers' function is to hold a finite amount of data. The extra information in a buffer can overflow into the next pad, and as a result, the valid data held in them will be corrupted or overwritten. Hence, attackers can interfere with the code and perform their aims. Another concern is the input validation process, designed to ensure that input data follows specific rules. If data validation is done incorrectly, data corruption, such as SQL injection, can occur. For example, a cybercriminal can inject SQL commands from the web to change a target database's content or get sensitive information such as passwords or credit cards.

2.2.3. Network infrastructure and protocols

Common network attacks have been exploiting the limitation of the network protocols Internet Protocol (IP), Transmission Control Protocol (TCP), and Domain Name System (DNS) (Cárdenas *et al.*, 2008). Secure Sockets Layer/Transport Layer Security (SSL/TLS) was developed to provide end-to-end security between two computers that sit over TCP. DNS protocol translates hostnames readable by humans into 32-bit IP addresses. So, the Internet tells routers which IP address to direct packets when a user gives a URL. However, DNS replies are not authenticated, and attackers can send malicious messages to access an Internet server (Kamal and Issac, 2007). A successful attack against DNS would disrupt communication on the Internet. Therefore, DNS has often been the target of Denial-of-Service attacks (DoS). These cyber-attacks flood web servers, networks, and systems with traffic that destroys victims' resources, and consequently, nobody else can access them.

3. THE IMPORTANCE OF HUMAN FACTORS

The digital transformation and innovative developments in information sciences do not always produce more secure environments. The impact of human factors in the failure to secure and protect systems, services, organizations, and information is enormous (Orshesky, 2003). Kearney highlighted that IT systems will become weak and can be exploited repeatedly by attackers as

long as security holes are overlooked by the process designers (Kearney, 2010). Hence, cybersecurity threats cannot be understood only by technical issues. Individuals operate computers and other (inter)-connected devices; this means that the security of such devices and environments is also a matter of human and organizational factors (O'Neill, 2014). In many cases, the adoption of security technologies has failed to protect organizations from cyberattacks (Anwar *et al.*, 2017). Human and organizational factors can be related to computer and information security vulnerabilities (CIS). Accordingly, Kraemer et al.'s findings suggested that these factors play a significant role in developing CIS vulnerabilities (Kraemer, Carayon, and Clem, 2009). In addition, they classified them in 9 areas: external influences, human error, management, organization, performance and resource management, policy issues, technology, and training. Other researchers agreed with the previous authors, and they represented these factors in two major groups (Badie and Lashkari, 2012):

- Factors belonging to the user: risky behavior, belief, lack of motivation, inadequate use of technology.
- Factors belonging to management: workload, inadequate staffing.

People may deny using security technologies, fail to follow the security protocols, engage in harmful activities that cause significant threats for them and organizations, and underestimate the chances of being victims of a cybersecurity breach (Herath and Rao, 2009). Because of these challenges, exploring and studying the role of human factors in cybersecurity has been of great interest. Human factors significantly influence people's interaction with information security, and therefore, they can pose many risks (Parsons *et al.*, 2010). Also, other authors highlight the importance of human factors in computer security (Metalidou *et al.*, 2014). Their study explained how human weaknesses could lead to the unintentional detriment to the organization and showed an increase in awareness level could help reduce these weaknesses.

Several research studies have indicated that security solutions that only go around hardware and software are unsuccessful (Crossler and Bélanger, 2014; Alohali *et al.*, 2017; Ratchford and Wang, 2019). The authors argued that an effective and flexible human factors methodology must be integrated into development processes (Pattison and Stedmon, 2006). It is of great interest to investigate the users' behaviors that lead to security risks when studying the human factor. Accordingly, Tu et al. highlighted that mobile devices' security solutions should focus more on the users' behavior than technical problems (Tu *et al.*, 2015).

A study comparing college students' and IT professionals' security behaviors showed that almost all the groups put themselves at risk by failing to secure their mobile devices properly (Oberlo, 2020). Additionally, the authors stated that security issues would not appear if users' behaviors were in line with security and protection. However, a study found that individuals make "quid pro quo" when weighing different security behaviors and do not always choose the optimal security-related option (Jeske, Briggs, and Coventry, 2016). Among the best practices against the threats posed by device proliferation, Romer suggests that if users monitor what applications use and install, the data security breaches will not be an issue (Romer, 2014). Likewise, authentication tokens have been suggested as helpful data security solutions (Steiner, 2014). Besides the relevant literature and suggested practices, there is a lack of research to study users' security behaviors and apply them correctly (Wang, Duong, and Chen, 2016). The human side is complex, and studies have shown that sometimes it is overlooked. As Thaler suggests, the behavior side should be viewed seriously (Thaler, 1980). Hoskin states that decision-makers can be more concerned about out-of-pocket losses than whether they have made the right decision from all the opportunities (Hoskin, 1983). From the viewpoint of IT security, choosing security leads to giving up on other options. And the question that logically follows is "Was it better?". Therefore, all costs in the IT Security field should be considered as opportunity ones too. Organizations take measures, and still, the accidents continue to occur. Studies have shown that programs related to employment training and people awareness are being integrated, but the situation is critical. Humans do not make any random movement; everything serves the purpose of "adapting" to the systems and external conditions. Apart from how intelligent an individual might be, the action still satisfies a general principle. "The ends justify the means," and people want to have better security, feel safe, and take such steps for better means. But do they know, understand, and apply what is better? While considering and analyzing the human side, it should also shed light on some critical factors related to cultural differences. Fukuyama explains why some societies do better than others, and he emphasizes the level of trust inherent in the community and social virtues differences between nations (Fukuyama, 1995). Thus, it is necessary to count, understand, and work with the human side and its influencing factors for better outcomes.

4. CONCLUSIONS

Technology is changing at a staggering rate. Since our dependence on information technology has been increasing, cyber-attacks are becoming more and more attractive. In some cases, cyberattacks have no vast impacts, but if they are done against critical infrastructure could have sufficiently significant effects on security on the national level, economy, life, and safety of peoples. Therefore, an infrequent successful attack with a huge impact can present a more considerable risk than an ordinary attack with low influence. Our research has stressed the importance of human factors in cybersecurity. Besides security solutions, technology alone cannot provide full support for cyber-attacks. We presented cybersecurity risks and identified human weaknesses causing security issues. It was shown that human factors significantly influence individuals' interaction with cybersecurity. Hence, it is proposed that understanding the human side is the key to mitigating security risks associated with human characteristics. The evidence from this work points toward the idea that the collaboration of private, public organizations, and academia is needed to cultivate positive security behaviors.

REFERENCES

Alohali, M. *et al.* (2017) *Information security behavior: Recognizing the influencers*. DOI: 10.1109/SAI.2017.8252194.

Andress, J. (2011) 'Chapter 1 - What is Information Security?', in Andress, J. (ed.) *The Basics of Information Security*. Boston: Syngress, pp. 1–16. DOI: https://doi.org/10.1016/B978-1-59749-653-7.00001-3.

Anwar, M. *et al.* (2017) 'Gender difference and employees' cybersecurity behaviors,' *Computers in Human Behavior*, 69, pp. 437–443. DOI: 10.1016/j.chb.2016.12.040.

Australian Parliament. House of Representatives (2010) *Hackers, fraudsters and botnets: tackling the problem of cybercrime: the report of the inquiry into cybercrime / House of Representatives, Standing Committee on Communications.* Canberra: Canberra : [The Committee].

Badie, N. and Lashkari, A. H. (2012) 'A new Evaluation Criteria for Effective Security Awareness in Computer Risk Management based on AHP,' *Journal of Basic and Applied Scientific Research*, 2(9), pp. 9331–9347.

Bayer, U. *et al.* (2009) 'A View on Current Malware Behaviors,' in *Proceedings of the 2nd USENIX Conference on Large-Scale Exploits and Emergent Threats: Botnets, Spyware, Worms, and More*. USA: USENIX Association (LEET'09), p. 8.

Cárdenas, A. A. *et al.* (2008) 'Cyber Security Basic Defenses and Attack Trends', in *Homeland Security*, pp. 73–103.

Chakraborty, R. S., Narasimhan, S. and Bhunia, S. (2009) 'Hardware Trojan: Threats and emerging solutions,' in *2009 IEEE International High-Level Design Validation and Test Workshop*, pp. 166–171. DOI: 10.1109/HLDVT.2009.5340158.

Cloudflare (2020) *What is a phishing attack?*

Cluley, G. (2010) 'Sizing up the malware threat – key malware trends for 2010', *Network Security*, 2010(4), pp. 8–10. DOI: https://doi.org/10.1016/S1353-4858(10)70045-3.

Crossler, R. and Bélanger, F. (2014) 'An Extended Perspective on Individual Security Behaviors: Protection Motivation Theory and a Unified Security Practices (USP) Instrument,' *SIGMIS Database*, 45(4), pp. 51–71. DOI: 10.1145/2691517.2691521.

Cybersecurity Insiders (2020) *2020 Insider Threat Report*. Available at: https://www.cybersecurity-insiders.com/wp-content/uploads/2019/11/2020-Insider-Threat-Report-Gurucul.pdf (Accessed: 15 September 2021).
FBI (2015) *Hurricane Katrina Fraud* . Available at: https://www.fbi.gov/history/famous-cases/hurricane-katrina-fraud (Accessed: 15 September 2021).
Fukuyama, F. (1995) *Trust: The Social Virtue and the Creation of Prosperity*. London: Penguin Books.
Herath, T. and Rao, H. R. (2009) 'Protection motivation and deterrence: a framework for security policy compliance in organizations', *European Journal of Information Systems*, 18(2), pp. 106–125. DOI: 10.1057/ejis.2009.6.
Herjavec Group (2020) *The 2020 Official Annual Cybercrime Report* . Available at: https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/ (Accessed: 15 September 2021).
Hoskin, R. E. (1983) 'Opportunity Cost and Behavior', *Journal of Accounting Research*, 21(1), pp. 78–95. DOI: 10.2307/2490937.
ISO/IEC (2018) *ISO/IEC 27000:2018(en), Information technology — Security techniques — Information security management systems — Overview and vocabulary*. Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en (Accessed: 17 August 2020).
Jang-Jaccard, J. and Nepal, S. (2014) 'A survey of emerging threats in cybersecurity, *Journal of Computer and System Sciences*, 80(5), pp. 973–993. DOI: https://doi.org/10.1016/j.jcss.2014.02.005.
Jeske, D., Briggs, P. and Coventry, L. (2016) 'Exploring the relationship between impulsivity and decision-making on mobile devices, *Personal and Ubiquitous Computing*, 20(4), pp. 545–557. DOI: 10.1007/s00779-016-0938-4.
Kadena, E. (2018) 'Lack of cybersecurity education', in Tadeusz, Z. and Horzela, I. (eds) *Współczesne problemy zarządzania, obronności i bezpieczeństwa. T. 2*. Varsó: Akademia Sztuki Wojennej, pp. 83–90. Available at: https://www.teldat.com.pl/images/download/czasopisma/ASzWoj_Wspolczesne_problemy_zarzadzania_obronnoscia_i_bezpieczenstwa_2018.pdf.
Kadëna, E. and Kerti, A. (2017) 'Security Risks of Machine-to-Machine Communications', *HÍRVILLÁM = SIGNAL BADGE*, 8(1), pp. 95–115.

Kadena, E., Nguyen, H. P. D. and Ruiz, L. (2021) ‘Mobile Robots: An Overview of Data and Security, in *Proceedings of the 7th International Conference on Information Systems Security and Privacy - Volume 1: ICISSP*, pp. 291–299. DOI: 10.5220/0010174602910299.

Kamal, S. and Issac, B. (2007) ‘Analysis of network communication attacks’, *2007 5th Student Conference on Research and Development, SCORED*, (December). DOI: 10.1109/SCORED.2007.4451370.

Kanich, C. *et al.* (2008) ‘Spamalytics: An Empirical Analysis of Spam Marketing Conversion, in *Proceedings of the 15th ACM Conference on Computer and Communications Security*. New York, NY, USA: Association for Computing Machinery (CCS ’08), pp. 3–14. DOI: 10.1145/1455770.1455774.

Kearney, P. (2010) *Security The Human Factor*. IT Governance Publishing.

Kraemer, S., Carayon, P. and Clem, J. (2009) ‘Human and organizational factors in computer and information security: Pathways to vulnerabilities’, *Computers & Security*, 28(7), pp. 509–520. DOI: 10.1016/J.COSE.2009.04.006.

Kulikova, T. and Shcherbakova, T. (2021) *Q2 2021 spam and phishing report*, *Securelist*. Available at: https://securelist.com/spam-and-phishing-in-q2-2021/103548/ (Accessed: 20 September 2021).

Li, Q. *et al.* (2008) ‘Hardware Threat: The Challenge of Information Security, in *2008 International Symposium on Computer Science and Computational Technology*, pp. 517–520. DOI: 10.1109/ISCSCT.2008.217.

Liu, S. and Cheng, B. (2009) ‘Cyberattacks: Why, What, Who, and How’, *IT Professional*, 11(3), pp. 14–21. DOI: 10.1109/MITP.2009.46.

McGraw, G. (2006) ‘Software Security: Building Security In’, in *2006 17th International Symposium on Software Reliability Engineering*, p. 6. DOI: 10.1109/ISSRE.2006.43.

Metalidou, E. *et al.* (2014) ‘The Human Factor of Information Security: Unintentional Damage Perspective’, *Procedia - Social and Behavioral Sciences*, 147. DOI: 10.1016/j.sbspro.2014.07.133.

Neumann, A., Statland, N. and Webb, R. (1977) ‘Post-processing audit tools and techniques, in *Proceedings of the NBS Invitational Workshop*. Miami Beach, Florida: US Department of Commerce, National Bureau of Standards, pp. 11–3; 11–4. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nbsspecialpublication500-19.pdf.

O'Neill, M. (2014) 'The Internet of Things: do more devices mean more risks?', *Computer Fraud & Security*, 2014(1), pp. 16–17. DOI: https://doi.org/10.1016/S1361-3723(14)70008-9.
Oberlo (2020) *How Many People Have Smartphones?* . Available at: https://www.oberlo.com/statistics/how-many-people-have-smartphones (Accessed: 12 May 2021).
Orshesky, C. M. (2003) 'Beyond technology - The human factor in business systems', *Journal of Business Strategy*, 24, pp. 43–47. DOI: 10.1108/02756660310494872.
Parsons, K. *et al.* (2010) *Human Factors and Information Security : Individual , Culture and Security Environment*, *Science And Technology*. Edinburgh (AUSTRALIA). DOI: 10.14722/ndss.2014.23268.
Pattison, M. and Stedmon, A. (2006) 'Inclusive design and human factors: Designing mobile phones for older users', *PsychNology Journal*, 4, pp. 267–284.
Potlapally, N. (2011) 'Hardware security in practice: Challenges and opportunities, in *2011 IEEE International Symposium on Hardware-Oriented Security and Trust*, pp. 93–98. DOI: 10.1109/HST.2011.5955003.
Ratchford, M. M. and Wang, Y. (2019) 'BYOD-Insure: A Security Assessment Model for Enterprise BYOD', in *2019 Fifth Conference on Mobile and Secure Services (MobiSecServ)*, pp. 1–10. DOI: 10.1109/MOBISECSERV.2019.8686551.
Romer, H. (2014) 'Best practices for BYOD security, *Computer Fraud & Security*, 2014(1), pp. 13–15. DOI: https://doi.org/10.1016/S1361-3723(14)70007-7.
RSA (2021) *DRIVE-BY DOWNLOAD*. Available at: https://www.rsa.com/content/dam/en/case-study/asoc-drive-by-download.pdf (Accessed: 20 September 2021).
Schultz, E. E. (2006) 'Where have the worms and viruses gone?—new trends in malware', *Computer Fraud & Security*, 2006(7), pp. 4–8. DOI: https://doi.org/10.1016/S1361-3723(06)70398-0.
Shabut, A. M., Lwin, K. T. and Hossain, M. A. (2016) 'Cyberattacks, countermeasures, and protection schemes — A state of the art survey', in *2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA)*, pp. 37–44. DOI: 10.1109/SKIMA.2016.7916194.
Shahriar, H. and Zulkernine, M. (2012) 'Mitigating Program Security Vulnerabilities: Approaches and Challenges, *ACM Comput. Surv.*, 44(3). DOI: 10.1145/2187671.2187673.

Steiner, P. (2014) ‘Going beyond mobile device management, *Computer Fraud & Security*, 2014, pp. 19–20. DOI: 10.1016/S1361-3723(14)70483-X.
Thaler, R. (1980) ‘Toward a positive theory of consumer choice’, *Journal of Economic Behavior and Organization*, 1(1), pp. 39–60. DOI: 10.1016/0167-2681(80)90051-7.
Tsipenyuk, K., Chess, B. and McGraw, G. (2005) ‘Seven pernicious kingdoms: a taxonomy of software security errors’, *IEEE Security Privacy*, 3(6), pp. 81–84. DOI: 10.1109/MSP.2005.159.
Tu, Z. *et al.* (2015) ‘Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination’, *Information & Management*, 52. DOI: 10.1016/j.im.2015.03.002.
Wang, T., Duong, T. and Chen, C. (2016) ‘Intention to disclose personal information via mobile applications: A privacy calculus perspective’, *International Journal of Information Management*, 36, pp. 531–542. DOI: 10.1016/j.ijinfomgt.2016.03.003.
World Health Organization (2020) *WHO reports a fivefold increase in cyber attacks, urges vigilance*. Available at: https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance (Accessed: 15 September 2021).