Information & Security

Published since 1998

I. Tikanmäki & H. Ruoslahti
vol. 55, no. 3 (2024): 245-259
https://doi.org/10.11610/isij.5522

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Human Factors Make or Break Cybersecurity!

Ilkka Tikanmäki [1,2] (✉) *and Harri Ruoslahti* [1]

[1] *Laurea University of Applied Sciences, Espoo, Finland*
https://www.laurea.fi/en/

[2] *National Defence University, Helsinki, Finland*
https://maanpuolustuskorkeakoulu.fi/en/

Abstract:

Social engineering attacks often exploit human traits like trust or fear, targeting network devices and personnel. Human vulnerabilities often stem from carelessness, unintentional errors, or lack of awareness. This study investigates how these and other human factors influence cybersecurity while also recognising the role of technology. Threats due to human elements, such as social engineering, cognition, and organisational security cultures, and outside influences, e.g., intentional cybercrime and phishing, can be countered with cyber skills and training. This research looks at prior findings in the areas of individual differences, such as intelligence, cognition, personality traits, and personal cybersecurity behaviours. Organisational factors, such as resource allocation, legal requirements, and technology design, are critical components that influence cybersecurity. This study notes the interconnectedness of the fields of cybersecurity, privacy, and application security. Based on a review of project deliverables, this study highlights cognitive biases, compulsive internet usage, cyberloafing, and password vulnerabilities as significant recognised challenges. Additionally, the study delves into organisational implications, including the role of, e.g., organisational culture in risk mitigation and the impact of Bring Your Own Device policies on security. Ultimately, the findings underscore the importance of holistic approaches to cybersecurity, integrating human, organisational, technological, legal, and ethical considerations.

Article Info:

Received: 05 Sep 2024
Revised: 20 Oct 2024
Online: 04 Nov 2024

Keywords:

human factors, HF, social engineering, cybersecurity, cognitive, organisational culture

✉ E-mail: ilkka.tikanmaki@gmail.com; harri.ruoslahti@laurea.fi

Introduction

Cyber-attacks can be categorised into human-based social engineering and computer-based social manipulation that uses computers. Hacking often involves strong human aspects through social engineering, which involves interaction with people to gather their sensitive information by exploiting human traits like trust, fear, or helpfulness. These activities may include, e.g., pretexting, eavesdropping, shoulder surfing, tailgating, and dumpster diving. Phishing and baiting are examples of computer-based social engineering.[1]

Information security should always be considered holistically because human risk factors can also cause other risks to develop in the information/data of organisations.[2] Many social engineering attacks focus on network devices, network components, sensing components, client devices, clinical network information systems, enterprise information systems, data centres, data, buildings, and personnel.

Vulnerabilities caused by human factors include, for example, unintentional errors, lack of awareness, social engineering, and phishing. The utilisation of critical information access is often influenced by the human factor, and employee awareness can be enhanced by promoting appropriate cyber skills, training programs and by defining appropriate employee roles.

In the cybersphere, psychological factors are essentially associated with the social and psychological aspects of human nature and how these aspects can be affected. The definition of individual differences is the permanent psychological characteristics that separate one person from another. Intelligence and personality traits are among these qualities. In the last few years, there have been multiple studies conducted to examine the influence of individual differences on cybersecurity.[3,4]

Cybersecurity can become affected by various organisational aspects, and technologies should be designed and organised with the end user in mind. Cutting back on resources can result in an enterprise becoming highly vulnerable to cyber threats from an economic or financial perspective.

Each sector has specific or cross-cutting legal, regulatory, and ethical requirements, and the fields of cybersecurity and privacy are increasingly connected to them. The security of application software, for example, is the focus of application security (AppSec), which is a specialised area of cybersecurity.[5]

This study investigates the multifaceted human factors influencing cybersecurity, and its research question is: What human factors affect cybersecurity? This research question encompasses key areas of investigation that include the exploration of human behaviour, cognition, and organisational factors, as well as the examination of individual differences and their impact on cybersecurity practices.

The contribution of this study to theory is that it addresses the interconnected nature of human factors in cybersecurity and privacy. A contribution to practice is its notion of emphasis on the importance of holistic approaches when considering cybersecurity and countermeasures to cyber threats. Many current studies look at human factors and aspects with a narrower focus.

The contents of this article are organised as follows: The study begins with an introduction, and human factors in the literature provide the background for the research. The method used in this study is introduced in the methodology section, followed by the findings, and the conclusion section concludes the study.

Human Factors in Literature

People are prone to cognitive biases and are influenced, *inter alia*, by organisational culture. Humans have a variety of attributes that contribute to security. According to Gratian et al., "humans are often identified as the weakest link in cybersecurity, as all technical security solutions are still susceptible to failure due to human error."[6] The complexity of mental abilities can lead to systematic errors in thinking that affect decision-making and judgments, known as cognitive biases.[7]

An organisation can foster a supportive work environment and reduce poor risk perception by adopting a 'no-blame' culture.[8] Compulsive use of the internet has been directly linked to a decrease in productivity[9,10,11] and an increase in cybersecurity breaches.[12] Compulsive Internet use increases the risk of causing various cybersecurity incident.[13]

The use of a company email and internet services for personal use while working is known as 'cyberloafing.'[14] Indiscreet and complacent in identifying threats can be a result of this practice, leading to the possibility of malware spreading into a company's system.[15] To prevent this behaviour, it is important to educate, be aware of security, and develop an Acceptable Internet Use Policy (AIUP).[16] Traditional passwords continue to be the most used authentication method, even though there are many other options.[17] The compatibility of passwords on all servers and browsers rated high.[17]

Passwords are considered weak secrets when it comes to security. Phishing activities are a major vulnerability that can trick users into revealing their passwords using different attack methods.[18] Third parties can compromise the security of password databases, while fraudulent, malicious, accidental, or intentional using privileges associated with a specific user account without knowledge of policies can occur when privileges are misused.[19] Data security breaches are mostly caused by the abuse of privileged accounts.[20]

Social engineering is focused on individuals with access to information, who are manipulated to reveal confidential information or perform malicious attacks through influence and persuasion.[21] Extrovert people were more prone to breaking cybersecurity policies than those who were more neurotic and conscientious,[22,23] as safety behaviours are negatively correlated with impulsivity.[24] Impulsive persons may act spontaneously without taking into account the consequences and the act itself,[25] while an employee may even be willing and capable of deliberately sabotaging, cheating, or stealing organisational intellectual property.[26]

Vigilantism involves the illegal use of violence by private individuals who desire to enforce laws without the help of law enforcement.[24] Although data theft and denial of service attacks may not appear violent in the cyber world, they are still considered cyber vigilantism activities. The primary tool for cyber vigilantes achieving their goals are their hacking skills, which they use to perform data theft or denial-of-service attacks.

Bring Your Own Device (BYOD) is the term used to describe allowing employees to use their own mobile devices to work to access company systems, software, networks, or data. The benefits of BYOD for companies include increased productivity, reduced information technology (IT) and operational costs, improved employee mobility, and improved employee recruitment and retention. Despite these advantages, the trade-off is increased security risks or breaches and increased organisational liability.[27]

The advanced know-how and production development of European companies make them particularly vulnerable to industrial espionage threats.[28] The term hacktivism is used to describe the application of technology to advance a political agenda or promote social change.[29] The roots of it lie in the culture of hackers and hacker ethics, which frequently pertain to freedom of speech, human rights, or people's independence.

A fundamental right is to protect individuals in the processing of personal data. The General Data Protection Regulation (GDPR) aims to advance the implementation of freedom, security, justice, and economic union, as well as economic and social progress.[30]

Methodology

This study builds on the prior efforts of project European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations (ECHO) and is part of the current efforts of Dynamic Business Continuity: Resilience Assessment & AI-based solutions in project Dynamic Resilience Assessment Method including combined Business Continuity Management and Cyber Threat Intelligence solution for Critical Sectors (DYNAMO). This study is part of project efforts as a series of individual studies focusing on human factors in cybersecurity.

This is a desktop study of four deliverables of the ended project ECHO: D2.1 Sector Scenarios and Use Case Analysis, ECHO Multi-sector Assessment Framework, D2.3 Transversal Cybersecurity Challenges and Opportunities, and D3.6 ECHO Information Sharing Models. These four were selected as they were deemed to contain the most relevant content for the ongoing DYNAMO project on how human factors relate to and can promote dynamic resilience against cyber threats and issues.

This analysis of 674 pages of project ECHO deliverables aimed at understanding the implications for human behaviours for information security. Search words used included: human factors, personal, behaviour, and individual. Data collection was aided by entering relevant data into a Data Extraction Table (DET) created for this study. The DET included three main rows: human factors, behaviours, and examples of human factors. This DET was also used to facilitate the data analysis of this study.

Results

Based on the four project ECHO deliverables cybersecurity risks can arise from competition between individuals or groups for incompatible goals, scarce resources, or power, which can lead to denial of control to others. The emergence of operational ethnic conflicts is a result of deep-rooted socio-cultural issues, which have a strong positive correlation with political and cultural conflicts. The following table outlines the challenges of cyber security from the perspective of human factors as they appear in the analysed data set.

Table 1. Human factors in cybersecurity in ECHO sample deliverables.

Human factor	Behaviour	Examples
Cognitive	Cognitive bias	Systematic errors in thinking
	Risk perception	A supportive environment reduces risk perception
Behavioural	Locus on control	Control over the outcome of life events
	Internet addiction	Compulsive use of the internet
	Gambling	The necessity for money
	Cyber loafing	Company's email and internet use for personal use
	Shopping addiction	Commerce without information security concerns
	Password storage	Data stored in an unprotected file
	Password weakness	Compatibility of passwords on all servers and browsers
	Privilege abuse	Data security breaches
	Human error	Can lead to the accidental leak of sensitive data.
	Social engineering	Making users compromise information systems
Psychological	Job satisfaction	Level of satisfaction employees have with their job
	Stress, depression, and anxiety	
	Fear	

	Fatigue and burnout	Decreased work performance Employees are under pressure to take certain actions Apathy and indifference to cybersecurity risks
Individual differences	Impulsivity	Desire to act spontaneously
	Personality Traits	The way someone follows cybersecurity procedures
Organisational factor	Mis-communication	Misinterpretation or misunderstanding of information
	Insider threat	Person with authenticated access to infrastructure
	Political motives	Individuals with hidden financial or political motives
	Cyber vigilantism	The illegal use of violence by private individuals
	Inadequate or non-updated training	Employees won't be able to recognise or respond to potential or recent threats
	BYOD	Employees use their own devices with company systems
Technology designed and organised for the end user	Privileged accounts	Vulnerable to corruption
	Network design	Access internal networks without verifying authenticity
	Device tampering	Impact on safety, privacy, and operations in general
	Critical infrastructure leaks	Hacked key information on key complex systems
Economical and financial aspects	Financial squeezing	Morale and motivation can be impacted by cuts
	Corporate espionage	Cyberspace offers a low-risk environment for actors.

	Crypto jacking	Computing power use without permission
Legal, ethics and regulatory aspects	Applicability of International law in cyberspace	A fundamental right is to protect individuals in the processing of personal data.
	Shifting ethical values	Ethical values changing can lead to insider threat
	Non-compliance with data protection regulations and directives	Can have a significant impact on the operation's results
	Application security	Internal process modelling, role-based access control
Strategic/ societal	Geopolitical	Cyber-attacks may be motivated by political ideologies
	Defence policy	Different defence policies
	Cyber terrorism	Internet's use to instil fear and perform violent acts
	International relations	The integration of politics, economics, and law
	Fake news	Using social engineering and/or OSINT
	Hacktivism	Applying technology to advance a political agenda or promote social change.

As seen in Table 1, multiple human traits contribute to cybersecurity. Humans are prone to making errors, which is why they are often referred to as the weakest link in cybersecurity.[31] All technical security solutions are vulnerable to human error. The following sub-sections discuss human factors relevant to cybersecurity in more detail.

Cognitive and Behavioural

Results indicate that individuals can recognise the magnitude of security breaches through risk detection. Poor employee perception of risk can be mitigated with training and education that are supported by appropriate organisational structures and atmosphere. The belief that one has control over the outcome of life events is known as locus of control. Despite considerable technological data security barriers, human errors can still cause the greatest risk to a system. Human error can, for example, lead to accidental leaks of sensitive data.

The necessity for money to meet addictions, such as gambling or other needs is referred to as gambling and financial stress. Results also show that to get financial benefits, an employee may act against their organisation.

Cyberloafing is the term used to describe the voluntary use of a company's email and internet services for personal purposes while working. The possibility of malware spreading into a company system can arise from indiscreet and complacent identification of threats. Compulsive use of the Internet, referred to as Internet addiction, is considered a pathological disorder.

Results from the analysis of the chosen ECHO deliverables show that fostering a supportive work environment and reducing poor risk perception can be achieved by adopting a 'no-blame' culture within the organisation. A decrease in productivity and an increase in cybersecurity breaches has been directly linked to the excessive use of the internet. The risk of causing various cybersecurity incidents increases with excessive internet usage. Cognitive biases can occur due to the complexity of mental abilities, which can lead to systematic errors in thinking that impact decisions and judgments.

According to the analysed materials, detecting anomalies and monitoring employee cyber behaviour are strategies for reducing these above-mentioned threats. Preventing e.g., cyberloafing requires educating, being aware of security, and creating an Acceptable Internet Use Policy (AIUP).

Shopping addiction may lead to an individual to search for electronic commerce without considering information security concerns. To combat this behaviour, it is possible to detect it actively at the organisational level or impose sanctions as a preventative measure. If data is stored in a historical or unprotected file, password saving can pose a problem. Therefore, data leaks and cyber-attacks pose significant risks.

Mitigation techniques can include active detection or sanctioning of this behaviour. Although there are many other options, results indicate that traditional passwords are still the most used authentication method. Passwords are highly rated for their compatibility with all servers and browsers.

Many data security breaches are seen to be caused by misuse of privileged accounts. Users can be tricked into revealing their passwords with, for example, phishing, which is a major vulnerability that can be used through different attack methods. The security of password databases can be compromised by third parties or privileges may become misused or subject to fraud, maliciousness, accidentality, or other intentional misuse.

Psychological

Individuals with access to information are the focus of social engineering. The art of social engineering involves making users compromise information systems. To counter this threat factor, it is possible to train employees to recognise social engineering attacks, sensitise them to cybersecurity threats, and monitor employee behaviour to detect such attacks.

Poor job satisfaction, defined as the level of satisfaction employees have with their jobs, may threaten cyber security. This especially depends on the position of the employee. Security breaches, sabotage, or espionage campaigns can cause severe threats. Organisations can be harmed by blackmail or threats, or an employee can deliberately sabotage, cheat, or steal the intellectual property of an organisation. This threat can be minimised by detecting anomalies in employee cyber behaviours and establishing strict security policies.

Recognising that employees are human and susceptible to mental health issues is the first step toward helping individuals who experience stress, which for example, can cause depression or anxiety, and decrease one's work performance. Long-term repeated stress may cause physical exhaustion. Fatigue can be demonstrated as apathy and indifference to cybersecurity risks.

Engaging staff in joint team-building activities and conducting regular psychological and behavioural testing (especially for those working in critical and high-security areas) are ways to mitigate or combat these risks. However, mitigation measures can be hindered by employee non-compliance (pushback) regarding participating in the activities.

Individual Differences

Impulsiveness refers to the urge to take immediate action without considering the consequences or the act itself. Impulsiveness has a high negative correlation with safety behaviours. Impulsive employees may share sensitive information publicly or allow outside sources to access internal networks without verifying their authenticity. Individual differences influence how someone follows cybersecurity procedures. Results show that cybersecurity policies are more likely to be broken by extroverts than by neurotic or conscientious individuals. Companies can implement cybersecurity awareness programs and conduct activities for all employees. However, there is no actual way to change individual personalities.

Organisational Factors

The collection of security-related information, technical or human, can lead to loss, misinterpretation, misunderstanding, or underestimating risk levels. The size of the organisation has an impact on the risk of miscommunication, and hierarchical organisations seem to pose a greater risk. A malicious threat to an organisation that is caused by individuals with authenticated access to its digital infrastructure is known as an insider threat. These individuals may be either former or current employees, contractors, or business partners. Organisational security practices, and knowledge of information and computer systems may be used by insiders to create the threat. The categories of insider threats can be broken down into malicious and careless insiders.

One or more individuals (e.g., politicians, public decision-makers, managers, and policymakers) can have hidden financial, political, or other motives. Vigilantism describes individuals who use violence or illegal acts to enforce laws according to their interpretation and without the aid of official law enforcement. Despite the lack of violence in the cyber world, data theft and denial-of-service attacks are considered acts of cyber surveillance while using hacking skills to achieve their goals, e.g., data theft or denial-of-service attacks.

The results indicate that organisations are vulnerable due to the lack of awareness of threats. Employees may not be able to recognise or respond to potential or recent threats if they receive only a little or no training on them. Organisations need to ensure that the level of training is adequate, up-to-date, and comprehensive. Organisations are responsible for ensuring that the training personnel is actively involved in developing their competence.

The concept of Bring Your Own Device (BYOD) refers to workers' usage of mobile devices to access company systems, software, networks, or data. Companies can benefit from BYOD by increasing productivity, reducing IT and operational costs, and improving employee recruitment, mobility, and retention. However, BYOD may also lead to security breaches and increased organisational liability, despite its advantages, resulting in a trade-off between security risks and benefits.

Technology Designed and Organised for the End User

Results also indicate that privileged user accounts (such as local administrator accounts, domain administrator accounts, service accounts, and application accounts) are necessary for a secure system and can be vulnerable to corruption. Configuring other users of the system or software is a crucial part of these accounts. Prevention is the focus for reducing this risk, with systems being managed by competent and well-trained personnel and old accounts being disposed of on time. Adding more devices to the company's information system can increase its vulnerability. As the number of connected devices increases, so does the risk of IT disruptions. One method of reducing these risks is to streamline equipment. According to the findings, the most vulnerable machines to cyberattacks are often the oldest devices; thus, it is important to remove them from the systems before they pose too much of a threat.

Attacks and hacking of key information from complex organisational systems can result in very critical technology leaks (e.g., artificial intelligence, biotechnology, and nanotechnology). Complex systems can become attacked by hackers, who may have political or financial motives. Insisting on strong defence protocols, regular updates, and being aware of new and growing threats in cyberspace is crucial with such systems.

Medical device tampering, for example, can pose exceptionally grave risk factors with direct impacts on patient safety and privacy. General hospital operations may become threatened and used as a bridgehead to the hospital network. The mitigation of this vulnerability involves ensuring that medical devices are updated regularly and training all individuals involved in using and calibrating them to ensure that these technologies can be used safely to care for patients.

Economic and Financial Factors

Table 1 also indicates that the impact of financial squeezing on a company can be significant and may predict future problems in the organisation. The majority of corporate or industrial espionage occurs in cyberspace, which offers a low-risk environment for industrial espionage threat actors. The risk of cyber corporate espionage can be significantly reduced by managing the identified problems, which increase the operational costs of threat actors.

Crypto-jacking is when a person or persons uses their computing power without permission to extract cryptocurrencies. The process of crypto mining involves validating transactions and adding them to the blockchain ledger. Prevention is key to preventing crypto jacking. Advanced intrusion prevention systems and next-generation firewalls are essential for acting at the firewall level.

Legal, Ethics, and Regulatory Aspects

The strengthening and convergence of internal market economies also impact the well-being of natural persons. Ethical values may change due to health problems, financial problems, disbelief in justice, depression, and other issues, which can lead to insider threats. The results recommend implementing internal controls and Segregation of Duties (SoD) that reduce the risk of fraud or errors impacting critical operations or resources of a company or organisation.

Complying with laws and regulations, and making changes to privacy and data protection can have significant impacts on operational results. New regulatory issues/requirements, including the EU General Data Protection Regulation (GDPR), may be involved with the expansion and growth of goals into several new sectors. The United Nations (UN) working groups have conversed about whether international law pertains to cyberspace and how states will apply their international rights and obligations. State obligations related to its activities in cyberspace can be reversed if there is a disagreement about the applicability of international law in cyberspace.

The development and refinement of Application Security (AppSec) practices are made possible by understanding the problem space faced by AppSec professionals. All possible AppSec threats cannot be addressed by a single solution. Addressing risks can be achieved through security from a multi-perspective perspective. Effective internal process modelling, and bulletproof role-based access control are necessary to counter any imminent AppSec threats due to most threats coming from current or former employees.

Strategic and Societal

Cyberterrorism involves using the internet to instil fear and perform violent acts that may result in the loss of life or significant bodily harm. Political or ideological gain is the goal of threats or harassment. Geopolitical motives have a significant impact on risk. Cyber-attacks may be motivated by political ideologies, whether initiated by cyber activists, a single attacker, or a large group of people. The indicators for operational risk are political activity, participation in warfare, financial investments, and legislation. Actively monitoring cyber-terrorists should be a priority. International collectives and national policies may have different defence policies. Many policies need to be adhered to by organisations, which can be problematic due to the difficulty of navigating and enforcing too many regulations. There are no technical solutions designed to specifically mitigate the risk of cyberterrorism.

International relations encompass the interaction between various nations around the world and the integration of politics, economics, and law at a global level. Fake news is connected to social media using social engineering and/or open-source intelligence (OSINT). One risk factor is that artificial information can be used to create fake trends that can manipulate people's opinions and generate the reaction and movement that the creator desires. Hacktivism is a blend of the words "hacking" and "activism". The term hacktivism describes the use of technology to advance a political agenda or foster social change. Hacker culture and ethics often relate to freedom of speech, human rights, or people's independence.

Conclusions

The study concludes that human factors play a crucial role in cybersecurity; however, most studies have focused on them as separate traits. The analysis of the four ECHO deliverables summarises human vulnerabilities, such as social engineering, lack of awareness, cognitive biases, etc., which all have a significant impact on cyber security outcomes. Combinations of these need to be considered when addressing cybersecurity measures and education.

The results suggest strategies to enhance cybersecurity. These include improving cybersecurity skills training, fostering a supportive organisational culture, and focusing on individual behavioural factors. Furthermore, the results underlie the connection between cybersecurity and privacy with the need for a comprehensive approach that encompasses technology, organisations, and legal factors to effectively safeguard against cyber threats.

Though based on a limited sample of practical applied materials, this study contributes to the theory of the complex interplay between the different human factors and cybersecurity. The crucial role played by social engineering tactics, cognitive biases, and organisational culture in exploiting cybersecurity vulnerabilities becomes emphasised. The contribution to theory by this study is that it recognises the interconnected nature of human factors when building awareness and countermeasures to cybersecurity.

This analysis of the ECHO project deliverables has helped understand the multifaceted nature of human behaviour and its implications for information security. This provides a contribution to practice as a summary used to guide further project efforts. Another contribution to practice is the emphasis on the importance of holistic approaches when considering cybersecurity education and training. The results of this study stress the importance of holistic approaches to cybersecurity with the need to address both technical and human-centric aspects.

According to the findings, it is important to create organisational procedures, guidelines and culture that promote cyber skills, cybersecurity awareness, and proactive risk management practices. Organisations can effectively mitigate threats and enhance resilience against cyber-attacks by tailoring cybersecurity strategies to consider individual differences, such as personality traits and cognitive abilities.

Furthermore, this study emphasises the significance of addressing new challenges, BYOD policies and industrial espionage threats have been named, in the context of cybersecurity governance and regulatory compliance. Organisations can protect sensitive information from malicious actors and uphold fundamental rights by aligning cybersecurity initiatives with legal and ethical frameworks.

To conclude, this research enhances understanding of the human aspects of cybersecurity and offers valuable insights for policymakers, industry practitioners, and cybersecurity professionals. Organisations can strengthen their defences and adapt to the changing threat landscape by incorporating human-centred approaches into cybersecurity strategies.

It is most important to ensure the confidentiality, integrity, and availability of critical information assets in an increasingly interconnected world. There are novel forms of social engineering, such as i.e., deepfakes, watering holes, and the very advanced possibilities brought about by novel developments in artificial intelligence, which were not addressed in this study, as they did not appear in the analysed materials. This only shows how very rapidly the sector is evolving. Therefore, further study on the role of human factors in cybersecurity against the ever-evolving novel strategies, solutions and technologies that can be used to take advantage of individuals and groups of people is recommended.

Acknowledgements

Acknowledgement is paid to the ECHO project, funded by the European Union Horizon 2020 research and innovation programme under grant agreement no. 830943, and the DYNAMO Project, under grant agreement no. 101069601. Views and opinions expressed are those of the authors only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them.

References

[1] Fatima Salahdine and Naima Kaabouch, "Social Engineering Attacks: A Survey," *Future Internet* 11, no. 4 (2019): 89, https://doi.org/10.3390/fi11040089.

[2] ISO, "ISO/IEC 27001 Standard – Information Security Management Systems," 2022.

[3] Mohd Anwar, Wu He, Ivan Ash, Xiaohong Yuan, Ling Li, and Li Xu, "Gender difference and employees' cybersecurity behaviors," *Computers in Human Behavior* 69 (2017): 437–43.

[4] Agata McCormac, Tara Zwaans, Kathryn Parsons, Dragana Calic, Marcus Butavicius, and Malcolm Pattinson, "Individual differences and information security awareness," *Computers in Human Behavior* 69 (2017): 151–6.

[5] Christopher Horn and Anita D'Amico, "Measuring Application Security," in *Advances in Human Factors in Cybersecurity*, edited by Ahram Tareq Z., Nicholson Denise (Cham: Springer, 2019), 44–55.

[6] Margaret Gratian, Sruthi Bandi, Michel Cukier, Josiah Dykstra, and Amy Ginther, "Correlating human traits and cyber security behavior intentions," *Computers & Security* 73 (2018): 345–58, https://doi.org/10.1016/j.cose.2017.11.015.

[7] Jordan Shropshire, Merrill Warkentin, and Shwadhin Sharma, "Personality, attitudes, and intentions: Predicting initial adoption of information security behavior," *Computers & Security* 49 (2015): 177–91.

[8] ENISA, "Cyber Security Culture in Organisations," February 06, 2018, www.enisa.europa.eu/publications/cyber-security-culture-in-organisations.

[9] Md Belal Ahmad, Ajhar Hussain, and Firoz Ahmad, "The use of social media at work place and its influence on the productivity of the employees in the era of COVID-19," *Sn Business & Economics* 2, no. 10 (2022): 29, https://doi.org/10.1007/s43546-022-00335-x.

[10] Mukhtar Al-Hashimi, Anjum Razzaque, Allam Hamdan, Sameh Reyad, Sherine Badawi, and Araby Madbouly, "The Impact of Internet Addiction on Bahraini Employees' Performance," *Lecture Notes in Networks and Systems* 194 (2021): 142–52, https://doi.org/10.1007/978-3-030-69221-6_11.

[11] David N. Greenfield and Richard A.Davis, "Lost in cyberspace: the web @ work," *Cyberpsychol Behav* 5, no. 4 (2002): 347–53, https://doi.org/10.1089/109493102760275590.

[12] Terrance Weatherbee, "Counterproductive use of technology at work: Information & communications technologies and cyberdeviancy," *Human Resource Management Review* 20, no. 1 (2010): 35–44, https://doi.org/10.1016/j.hrmr.2009.03.012.

[13] Raymond R. Panko, *Corporate Computer and Network Security*, 2nd edition (Boston: Pearson College Div; 2009).

[14] Emily Lowe-Calverley and Rachel Grieve, "Web of deceit: Relationships between the dark triad, perceived ability to deceive and cyberloafing," *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 11, no. 2 (2017), https://doi.org/10.5817/CP2017-2-5.

[15] Lee Hadlington and Kathryn Parsons, "Can Cyberloafing and Internet Addiction Affect Organizational Information Security?" *Cyberpsychol Behav Soc Netw* 20 no. 9 (20179): 567–71, https://doi.org/10.1089/cyber.2017.0239.

[16] Daniele Vernon-Bido, Gayane Grigoryan, Hamdi Kavak, and José Padilla, "Assessing the Impact of Cyberloafing on Cyber Risk," *Proceedings of the Annual Simulation Symposium, San Diego, CA, USA: Society for Computer Simulation International*, 2018, pp. 1–9.

[17] Joseph Bonneau, Cormac Herley, Oorschot Paul C. Van, and Frank Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," *2012 IEEE Symposium on Security and Privacy,* IEEE, 2012, pp. 553–67.

[18] Klaudia Krawiecka, Arseny Kurnikov, Andrew Paverd, Mohammad Mannan, and N. Asokan, "SafeKeeper: Protecting Web Passwords using Trusted Execution Environments," *Proceedings of the 2018 World Wide Web Conference* Republic *and Canton*

of Geneva, *CHE: International World Wide Web Conferences Steering Committee*, 2018, pp. 349–58.

[19] Jeff Melnick, "Privilege Abuse: Threat Alert," *Https://BlogNetwrixCom/*, 2017, accessed February 11, 2024, https://blog.netwrix.com/2017/10/24/privilege-abuse-threat-alert/,.

[20] Verizon, *2019 Data Breach Investigations Report* (New York, NY, USA: Verizon, 2019).

[21] Katharina Krombholz, Heidelinde Hobel, Markus Donko-Huber, and Edgar Weippl, "Advanced social engineering attacks," *Journal of Information Security and Applications* 22 (2014): 1–11, https://doi.org/10.1016/j.jisa.2014.09.005.

[22] Jeyhun Hajiyev and Basil John Thomas, "The Direct and Indirect Effects of Personality on Data Breach in Education Through the Task-Related Compulsive Technology use: M-Learning Perspective," *IJCDS* 9, no. 3 (2020): 459–69, https://doi.org/10.12785/ijcds/090310.

[23] Maranda McBride, Lemuria Carter, and Merrill Warkentin, *Exploring the Role of Individual Employee Characteristics and Personality on Employee Compliance with Cybersecurity Policies* (Washington D.C.: Department of Homeland Security, 2012).

[24] Jeff Kosseff, "The hazards of cyber-vigilantism," *Computer Law & Security Review* 32, no. 4 (2016): 642–9, https://doi.org/10.1016/j.clsr.2016.05.008.

[25] Mary Aiken, *The cyber effect: a pioneering cyber-psychologist explains how human behavior changes online* (New York: Spiegel & Grau, 2016).

[26] Michael G.Gelles, *Insider threat: Prevention, detection, mitigation, and deterrence* (Butterworth-Heinemann, 2016).

[27] Abubakar Bello Garba, Jocelyn Armarego, David Murray, and William Kenworthy, "Review of the Information Security and Privacy Challenges in Bring Your Own Device (BYOD) Environments," *Journal of Information Privacy and Security* 11, no. 1 (2015): 38–54, https://doi.org/10.1080/15536548.2015.1010985.

[28] Peter Krapp, "Terror and Play, Or What Was Hacktivism?" *Grey Room* 21 (2005): 70–93, https://doi.org/10.1162/152638105774539770.

[29] Eric Conrad, Seth Misenar, and Joshua Feldman, "Domain 1: Security and Risk Management," Chapter 2 (e.g., Security, Risk, Compliance, Law, Regulations, Business Continuity), in Conrad Eric, Misenar Seth, Feldman Joshua, eds., *CISSP Study Guide,* 3rd edition (Boston: Syngress, 2016), pp. 11–79.

[30] European Parliament and the Council, "General Data Protection Regulation (GDPR)," 2016.

[31] Harri Ruoslahti, Janel Coburn, Amir Trent, and Ilkka Tikanmäki, "Cyber Skills Gaps – A Systematic Review of the Academic Literature," *Connections: The Quarterly Journal* 20, no. 2 (2021): 33–45, https://doi.org/10.11610/Connections.20.2.04.

About the Authors

Ilkka **Tikanmäki** – see the CV on p. 78 of this volume, https://doi.org/10.11610/isij.5523. https://orcid.org/0000-0001-8950-5221

Harri **Ruoslahti** – see the CV on p. 78 of this volume, https://doi.org/10.11610/isij.5523. https://orcid.org/0000-0001-9726-7956