SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2023
ORGANIZATION AND MANAGEMENT SERIES NO. 184

IDENTIFYING CYBERRISK FACTORS IN HYBRID WORKFORCE ENVIRONMENTS

Krzysztof PRZYBYSZEWSKI[1], Karolina MAŁAGOCKA[2*], Zofia PRZYMUS[3]

[1] Department of Social Psychology, Kozminski University, Warsaw, Poland; crispy@kozminski.edu.pl, ORCID: 0000-0001-8271-9155
[2] Department of Marketing, Kozminski University, Warsaw, Poland; kmalagocka@kozminski.edu.pl, ORCID: 0000-0003-2544-2094
[3] Department of Management, Kozminski University, Warsaw, Poland; coercion@kozminski.edu.pl, ORCID: 0000-0003-2450-3932
* Correspondence author

Purpose: This academic paper addresses the impact of cyberattacks on companies, employees, and customers, particularly in the context of increased digitalization due to the pandemic. It emphasizes the importance of the human factor in cybersecurity and proposes the need for a universal tool to measure threat perception and behaviour tendencies. The paper aims to expand knowledge in measuring employee exposure to cyberthreats, especially in remote and hybrid work, by presenting methodology, findings and applications.
Research Background: In recent years, cybersecurity has gained significant attention, with a surge in published articles focusing on technical aspects and the human factor. However, there is a research gap regarding potentially dangerous behaviour among employees in remote or hybrid work models. Understanding individual differences in perceptions of cybersecurity is crucial for identifying vulnerabilities and enhancing corporate cyber resilience.
Methods: A qualitative pilot study was conducted to create the "Employees' Exposure to Cyberthreats Scale" based on interviews with cybersecurity professionals. The scale was then validated through a survey study with a representative sample of remote employees (N = 563). The questionnaire employed an expectancy approach, assessing severity and probability of unsafe behaviours on a 5-point scale.
Findings & Value Added: This paper presents the development and validation of a cyber exposure scale, measuring general and specific categories of cyberexposure. Three behaviour categories emerged: environmental, credential-related, and behavioural. The study provides preliminary results and practical implications for organizations to enhance cyber resilience, emphasizing the importance of employee behaviour and attitudes for cybersecurity practices. The findings contribute to tailored security policies and the development of a cybersecurity-focused organizational culture.
Originality/value: This research addresses a gap in the current cybersecurity literature by focusing on the behaviors and perceptions of employees in remote and hybrid work models, an area which has seen increased relevance due to the pandemic-induced shift to digital platforms. Introducing the 'Employee Cyber Threat Exposure Scale', this paper provides a tool to measure individual differences, offering organisations insights to strengthen their cyber resilience.

Keywords: cybersecurity; cyber resilience; remote work; cyber behaviours; digital transformation.

Category of the paper: Research paper.

1. Introduction

The number of cyberattacks increases every year, and the phenomenon has only intensified due to the pandemic and the shift of most users to the virtual channel. According to McKinsey (2022), the pandemic has accelerated the average share of fully digitalized products and services by seven years globally and in the case of customer interactions by three years. This means that growing numbers of companies, their employees, as well as users and customers, are operating in the digital channel, implying that the attack surface has increased. This is visible in the number of recorded hacking attacks and data leaks that are regularly reported by the global media.

The organisation of companies' vulnerability to cybercrime and the prevention of attacks has increasingly focused on the human factor. A significant amount of the academic literature related to information security has shifted its focus from the technological aspect to considering the role of employee attitudes and behaviours. Researchers dealing with the relationship between humans and cybersecurity noted a general discrepancy between actual behaviour and awareness or knowledge of rules, although no separate research was devoted to this issue (Bada, Sasse, Nurse, 2019; Hong, 2023; Pratama, Alshaikh, Alharbi, 2023; Zwilling et al., 2022. There is a paucity of literature on the subject of worker exposure to cyberthreats. Additionally, most studies use separate scales for measuring behaviour and attitudes, while in our study we suggest a synergy of both approaches and the creation of a universal tool for analysing the perception of threats, tendencies toward specific behaviours and the aggregation of both of the above values. In addition, the context appears to be important, which at the same time affects the novelty of the proposed project: it is highly embedded in reality, which is influenced by the COVD-19 pandemic and the related changes in the way work is performed, the use of devices, and the company's IT facilities, as well as the accelerated digital transformation of many organizations. The conducted research is motivated by the inability to provide security by using only technological solutions that fail if employees do not comply with cybersecurity rules, are against them, or even display risky behaviour (Anwar, He, Yuan, 2016; Hadlington, 2017; Bada, Nurse, 2019; Moustafa, Bello, Maurushat, 2021). The present study considers the relationships between the attitudes of employees towards problematic and thus potentially unsafe use of the Internet and devices, as well as their ability to engage in behaviours related to the security level of the corporate network and data (Alahmari, Duncan, 2020). The goal is to expand our knowledge of measurement tools for employees' exposure to cyberthreats.

The Risky Cybersecurity Behaviour Scale (RScB) (Egelman, Peer, 2015) and Attitudes Towards Cybersecurity and Cybercrime in Business (ATC-IB) (according to Hadlington, 2017) were developed in 2015 and 2016, respectively, taking into account the then-current conditions. The RScB Scale analyzed the specific types of "risky" cybersecurity practices users were involved, while another the ATC-IB Scale outlook on cybersecurity and their overall understanding of cybercrime. A novelty and contribution to the existing body of literature in our paper is the development of a measurement tool in line with the new cyberspace uses evolved after 2015 and 2016, and the evolution of technology. Our proposed scale is partially based on the previously developed tool (Egelman, Peer, 2015), and was created with input from digital forensic investigators and law enforcement. It includes behaviours that lead to poor cybersecurity practises that have caused companies to be attacked. The ATC-IB scale (according to Hadlington, 2017) was constructed based on expertise from the police, digital forensics, criminal psychology, and cyber psychology, to reflect a wide range of attitudes towards both cybersecurity and cybercrime within a business context. The present research verified the items contained in both measurement tools and adjusted them to the reality of changes in the rules of work (remote/hybrid) in connection with the COVID-19 pandemic. Remote working and intensifying social engineering attacks appear to be particularly important. The main aim of the research undertaken was to fill the research gap by:

- identifying and categorising items related to risky Internet and device use,
- expansion of the scale of hybrid and remote employees' exposure to cyberthreats.

The structure of this paper is as follows: firstly, it introduces the scope of research conducted so far, which takes into account the aspects of cybersecurity and the human factor, with particular emphasis on the tendency to engage in potentially risky behaviours. The methodology and methods of data analysis are then described. This is followed by a discussion of the research findings, their interpretation, and areas of application. Finally, the limitations and conclusions of this research are presented.

2. Literature review

The subject of cybersecurity is becoming a topic of interest for researchers, academics, and representatives of the business world. It should be emphasised that this is not a new phenomenon. In the Web of Science database, 12,164 articles containing the term 'cybersecurity' have appeared since 2010. The majority of them were published after 2017, while the limiting date after which more than 10 articles per year started to be published is precisely 2010. After applying publication date and journal category restrictions, 2256 articles were further analysed, with 182 papers being reviewed in detail at the end (description in Appendix 1). The bibliometric analysis demonstrates that the body of research is expanding,

however the great majority of them focuses on the technical aspect. Nevertheless, there are studies and conceptual works dedicated to the human factor in cyber security. Interest in the topic of cyber security can start by defining cyberspace as an expanding network structure (Ergen, Ünal, Saygili, 2021). The challenge is to accurately define cyberspace due to its growing global reach and the possibility of merging or interpenetrating different spheres, making its boundaries unrecognisable (Lu, Ye, Tan, 2023; Singer, Friedman, 2014). Cyberspace will provide a platform where resources such as individuals' digital lives, data, equipment, national infrastructure, or national systems become accessible without the barriers of physical space, which means that they are vulnerable to cyber-attacks and need to be protected (von Solms, von Solms, 2018). Meanwhile, in a rapidly changing reality, the development of technology, digital products and services represents a social aspect linked to the actions of users and, in the case of companies, and employees, is becoming increasingly important. Everyone should be aware of the cybersecurity risks and be prepared that individual actions may increase the risk, whereas proactive activities such as awareness-raising may reduce it. Hence, there is a demand for a reliable and valid instrument to measure cybersecurity practices and their perceptions.

Researchers have attempted to investigate how individual differences may affect a person's compliance with cybersecurity procedures and the risk behaviours manifested by them. Shropshire et al. (2006) and Panko (2010) noted that inappropriate use of computers, including using unauthorised applications or downloading files from unknown sources and visiting infected websites, is part of the catalogue of bad cyber-security behaviours, but called for further research to identify which aspects are technology-related. McBride, Carter and Warkentin (2012) found that more extroverted individuals were more likely to have cyber security breaches than more neurotic and conscientious individuals. Uebelacker and Quiel (2014) investigated the relationship between vulnerability to social engineering attacks and personality. Shropshire, Warkentin and Sharma (2015) demonstrated that the intention to use the new security software and the actual use of it were also due to diligence and agreeableness. In addition, there are several studies which associate different demographic characteristics with distinctive behaviours in cyberspace. Some researchers point to age as an important factor. According to their findings, younger people in the 18-29 age group are less aware of and more susceptible to attacks using social engineering techniques such as, inter alia, phishing compared to those over 30 (Arend et al., 2020; McCormac et al., 2017; Sağlam, Miller, Franqueira, 2023) Another variable is gender, which is also, in some studies, linked to different levels of cyber vulnerability. In this case, women are less aware, especially when it comes to data leakage attacks. On the other hand, they are more likely to update their software regularly and follow the rules of company security policies (Anwar et al., 2017; Gratian et al., 2018; Ünal, 2020). There is also a wave of research focused on conscientiousness, agreeableness, and openness (McCormac et al., 2017), which combines the above features with reduced risk-taking and increased awareness of good cybersecurity practices. Attitudes towards risk-taking appear to be

related to different dimensions of cyber security, according to research already conducted. Risk-taking folds into less safe online behaviour, while attitudes related to risk avoidance in the physical world (e.g. a deficiency of interest in extreme stunts) demonstrate a negative correlation with proactive protective behaviour in the cyber world (Hadlington, 2018). Subsequently, researchers are keenly and frequently exploring topics related to trust, as well as the perceived risk and security of specific technologies, such as the Internet of Things, mobile banking, but also the wider use of apps in everyday life (Kumar, Yukita, 2021; Merhi et al., 2020; Monfared et al., 2023). In addition to individual perceptions of risk, attitudes towards decision-making still appear to be important, which, as the authors point out, requires in-depth research and is one of the reasons for addressing this topic in the following article (Donalds, Osei-Bryson, 2020) Within the academic discourse on the relevance of the human factor in cyber security, there is also a theme of not mistreating users as enemies. In the literature, the most commonly stated reasons are related to the role of users as the first line of defence against cyber threats (Abawajy, 2014). Most cyber-attacks rely on tricking users into taking some action, such as clicking a malicious link or opening a phishing email. Educating users on how to recognize and avoid these types of attacks is an important part of protecting the organization. Treating users as enemies can also create a negative culture (Enescu, 2019). If users feel that they are constantly being blamed for security breaches or that their actions are being heavily monitored, it can create a negative and unproductive working environment.

Simultaneously, with the growing interest in the human factor, there is a gap in the scale for measuring potentially dangerous behaviour among employees working from home or in the hybrid model, taking into account the changes that have occurred in the application of technology since the introduction of the Risky Cybersecurity Behaviour Scale (RScB; Egelman, Peer, 2015) and Attitudes Towards Cybersecurity and Cybercrime in Business (ATC-IB, according to Hadlington, 2017), which were developed in 2015 and 2016, respectively. Meanwhile, research confirms that better individual differences regarding perceptions of cyber security can guide researchers, organisations, and those responsible for corporate cyber resilience to better understand vulnerabilities to potential attacks (Gratian et al., 2018).

3. The research

3.1. Eliciting list of cyberthreats

We conducted a qualitative pilot study to create the employees' exposure to cyberthreats scale, using the RScB and ATC-IB scales as the basis for the interview scenario. The study was conducted on a purposively selected sample of cybersecurity professionals (N = 11) and consisted of two stages: IDI and the selection of the final list of behaviours by competent judges.

A competent judge in scientific research methodology is an individual who is knowledgeable about the principles and practices of scientific research and is able to evaluate the quality and validity of research studies. It is generally expected that competent judges will have a good understanding of the relevant research methods and principles in their area of expertise (Wolfson, 1986). In the case of our study, they were people with more than 10 years of experience in the cybersecurity industry, involved in threat detection, identifying attack vectors, and designing appropriate security features to prevent them. In turn, the experts were people who had worked in the cyber security industry for less than five years and were involved in offering, implementing, and training company employees. Each of the experts and competent judges works for a different organization and, during the study, they did not communicate with each other regarding the judgements they made.

During the IDI, experts updated potentially dangerous behaviours, for example, by rejecting claims about downloading entertainment from the Internet, and adding behaviours as a result of remote working and the necessity of combining work and family responsibilities—such as lending work computers to children for online learning1. In total, the experts identified 57 potentially dangerous online behaviours, adequate for the digital transformation forced by the COVID-19 pandemic. Competent judges rated this list of behaviours on a 5-point Lickert scale, assigning a score of one to five, and shortened this list to the most dangerous. As a result, we received a 36-item scale of unsafe behaviour, which we used for quantitative research.

3.2. Construction of the scale

Overview

The preliminary list of 32 items from the pilot study was used to create a questionnaire based on the expectancy approach, which is widely used in motivation studies (Vroom, 1964) and attitude research (Fishbein, 1967; Ajzen, Fishbein, 1977; Ajzen, 2011). We contend that expectancy, defined as the composite of the subjective assessment of the severity of the threat (i.e., value) and the subjective assessment of the probability of a threatening behaviour being performed (i.e., probability), is the appropriate way to measure the risks associated with various employee actions.

The model applied to cyberthreats can be described by the following formula:

$$\boldsymbol{CE = ss_1 \times p_1 + \cdots + ss_i \times p_i}$$

where:

CE – Cyber exposure,

ss_i – subjective assessment of the severity of the threat,

p_i – subjective assessment of the probability of the threatening behaviour,

[1] The digital transformation caused by the COVID-19 pandemic was rapid and holistic—it concerned all aspects of life, including the need to bring education in schools online. There was a sudden shortage of computers on the market, and many families in Poland were forced to either (1) use private computers for business purposes or (2) lend computers to other household members.

Method

The idea of the scale to the subject was based on Exploratory Factor Analysis (EFA) approach, hence no a priori hypotheses concerning the structure of the scale were put forth. The factorial structure was to be elicited on the basis of the results of the survey study in which the participants evaluated the severity of the threats posed by online behaviours.

The questionnaire consists of two sets of items: (a) measuring the valence – subjective evaluation of the severity of the behaviours and (b) measuring the subjectively assessed probability of performing the behaviours. The severity of the threat: i.e. how big the threat of the following behaviour is? was measured with a 5-point scale ranging from 1= no threat at all to 5= very big threat. The probability of a threatening behaviour i.e. how probable is it that you perform the following behaviour was measured with a 5-point scale ranging from 1= zero probability to 5= very high probability.

The sample

The participants (N = 563) were a representative sample of employees who have experience working remotely, recruited from the biggest national internet research panel (Ariadna).

Results

The assessment of the general level of cyberthreats exposure.The first step in the factor analysis was to develop a one-factor cyber exposure scale that would allow for the calculation and indexing of general levels of exposure to cyberthreat. To achieve this, the list of 32 items measuring the severity of the behaviours was subjected to principal component factor analysis with Varimax rotation[2]. For the factor loadings see Table 1.

Table 1.
The factor loadings

	General cyber-exposure
Not using two-factor authentication for organization resources.	.816
Sending confidential data by e-mail without securing it with an additional password.	.813
Storing company information on personal electronic device (e.g. smartphone/tablet/laptop).	.812
Postpone updating any installed antivirus software.	.810
Downloading digital media (music, films, and games) from unlicensed sources.	.802
Downloading free software from an unknown source.	.802
Using free online file transfer service (e.g. WeTransfer).	.799
Not checking for updates of the used web browser.	.788
Downloading data and material from websites on work computer without checking its authenticity.	.777
Not locking the computer when leaving it. (e.g. no screensaver with a password).	.776
Postponing software updates on smartphone/tablet/laptop/computer.	.774
Disabling anti-virus software on work computer in order to be able to download information from websites.	.766
Using the same password for multiple websites.	.763
Having no antivirus program on the computer.	.762

[2] Varimax rotation is a typical factor analysis in psychology that allows the construction of a scale with orthogonal dimensions.

Cont. table 1.

Creating company documents in public places (e.g. when travelling by train or plane).	.761
Sharing a work computer or work phone with household members (e.g. using a work computer for online lessons).	.755
Conducting/participating in video conferences in public places.	.751
Using free-to-access public Wi-Fi.	.750
Using an unchanged (provided by the Internet provider) password on your home Wi-Fi.	.739
Using or creating passwords that are not very complicated. (e.g. family name and date of birth).	.733
Sending personal information to strangers over the Internet.	.733
Sharing current location on social media.	.729
Clicking on links contained in an email or social media message from a trusted friend or work colleague, even if they have strange content (e.g. "I'm in a contest, I need your vote").	.726
Using automatic password storage systems in your web browser.	.721
Using or creating passwords that do not include minimum standards (e.g. 8 characters minimum, upper- and lowercase characters, symbols).	.718
Create videoconferencing in free applications such as Zoom.	.709
Sharing your home Wi-Fi password with other people	.709
Relying on a trusted friend or colleague in terms of advice on aspects of online-security.	.698
Sharing password with trusted friends or colleagues.	.687
Clicking on links contained in unsolicited emails from an unknown source.	.686
Accepting friend requests on social media, after recognising the photo.	.670
Storing credit card numbers in shops that are rarely used.	.659

The scale is consistent, and all 32 items contribute to a single factor of general cyberexposure. One factor solution explains 56.4% of the variance and produces a highly reliable scale of Cronbach alpha = 97.

Results: The assessment scale of the specific levels of cyberthreat exposure

Reconstructing the natural categories of cybersecurity-related behaviours was the purpose of this part of our research. Factor analysis is a popular method for eliciting mental or perceptual structures. We assumed that for practical purposes (i.e. diagnosis, prevention and employees' training) the company would request a way of grouping the behaviours into some categories based on the way they are perceived by the employees. This led us to explore a multi-factor solution that would allow us to separately assess the cyberexposure arising from different categories of behaviours.

The list of 32 items (again the severity ones) was subjected to factor analysis, principal components method with Varimax rotation. The items with factor loadings below .50 were eliminated. Both the Kaiser criterion and the scree plot test corroborate the three-factor solution (see Appendix 2). The authors decided to give the factors names related to the main feature manifested in them, i.e. environmental, behavioural and The analysis revealed three factors accountable for 67% of the variance explained. The authors decided to give the factors names related to the main feature manifested in them, i.e. environmental, behavioural and credential-related. See Table 2 for the matrix of 26 items with their factor loadings.

Table 2.
The matrix of 26 rotated factors with their factor loadings

	Environmental	Behavioural	Credential-related
Create videoconferencing in free applications such as Zoom.	.825		
Conducting/participating in videoconferences in public places.	.817		
Creating company documents in public places (e.g. when travelling by train or plane).	.763		
Sharing a work computer or work phone with household members (e.g. using a work computer for online lessons).	.733		
Using free-to-access public Wi-Fi.	.693		
Not using two-factor authentication for organization resources.	.683		
Sharing current location on social media.	.634		
Accepting friend requests on social media, after recognising the photo.	.633		
Not checking for updates of the used web browser.	.629		
Not locking the computer when leaving it. (e.g. no screensaver with a password, etc.).	.622		
Postponing software updates on smartphone/tablet/laptop/computer.	.599		
Giving home Wi-Fi password to other people.	.555		
Clicking on links contained in unsolicited emails from an unknown source.		.844	
Sending personal information to strangers over the Internet.		.802	
Downloading data and material from websites on work computer without checking its authenticity.		.790	
Having no antivirus program on the computer.		.773	
Clicking on links contained in an email or social media message from a trusted friend or work colleague, even if they have strange content (e.g. "I'm in a contest, I need your vote").		.762	
Disabling anti-virus software on work computer in order to be able to download information from websites.		.652	
Postpone updating any installed antivirus software.		.632	
Storing company information on personal electronic device (e.g. smartphone/tablet/laptop).		.577	
Using or creating passwords that are not very complicated. (e.g. family name and date of birth).			.821
Using or creating passwords that do not include minimum standards (e.g. 8 characters minimum, upper- and lowercase characters, symbols).			.797
Sharing password with trusted friends or colleagues.			.779
Using the same password for multiple websites.			.756
Using online storage systems to exchange and keep passwords.			.682
Using an unchanged (provided by the Internet provider) password on your home Wi-Fi.			.596

The factor grouping the behaviours related to working online in unsafe places (and creating such unsafe places) was named *environmental* threats; the factor grouping the various types of misuse of *credentials-related* threats, and the careless behaviours and omission of preventive actions we decided to call *behavioural* threats.

The three sub-scales are highly reliable: for the *environmental* scale, Cronbach's alpha = 95, (2) for the *credentials*, Cronbach's alpha = 9, and (3) for the *behavioural*, Cronbach's alpha = 94.

3.3. Preliminary results of the application of the scale

The PMP's scale was distributed online (Ariadna panel) the representative sample of 563 employees with experience working remotely (the same sample as for the construction of the scale). To test the differences between three categories of threats (i.e. the *environmental*, the *credentials*, and the *behavioural*) repeated measures analysis of variance was conducted with the category of the threat as a within-subject variable, separately for severity and probability responses.

The analysis for severity revealed a statistically significant differences between various types of threats ($F(2, 1124) = 191.21$, $p < .000$; etasq = .25). The analysis for probability also revealed significant differences between the types of threats ($F(2, 1124) = 194.09$, $p < .000$; etasq = .26). The results are presented in Figure 1.

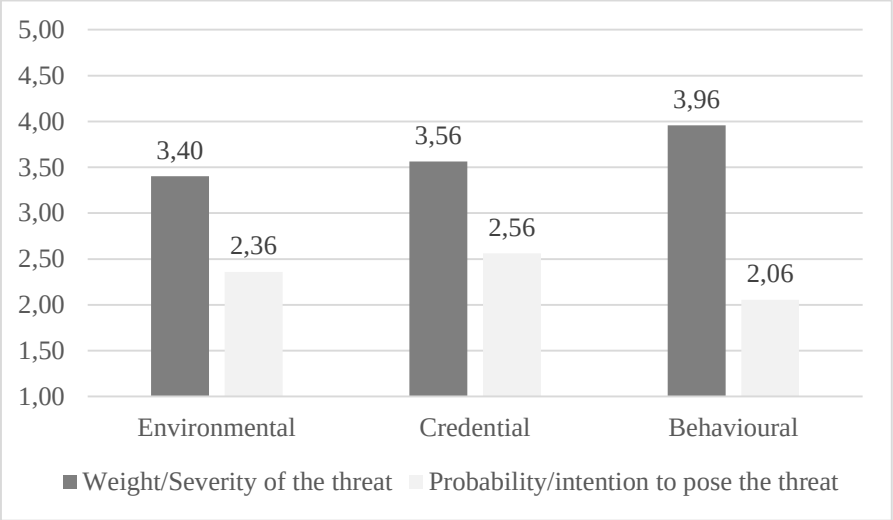

Figure 1. Mean severity and mean intentions to perform threat-posing actions.

According to Figure 1, threats related to the unprotected environment have the lowest severity, while behavioural threats (traditionally considered as such) have the highest severity (all differences significant at $p < .001$). The pattern for probability is also consistent with the notion of 'traditional' threats – the willingness to do so is the lowest (all differences are significant at $p < .001$).

The most useful in business practice is the analysis of the compound result—the risk posed by the employees to the company—calculated as an expected value. Repeated measures Anova revealed significant differences between the risk related to different types of behaviours elicited in our/PMP scale ($F(2, 1124) = 64.,12$, $p < .000$; etasq = .10). The mean values are presented in Figure 2.

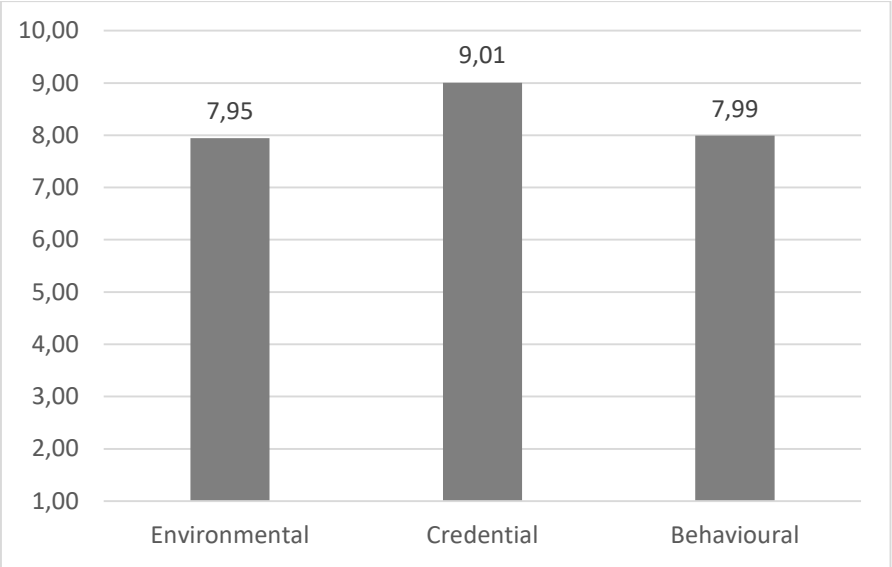

Figure 2. Mean values of risk posed by the employee's actions.

As can be seen, the highest value is 9.01, indicating the highest risk is associated with credential misuse, with the remaining factors a slightly lower. The results are interesting because the traditional risks (environmental and behavioural) appears to be quite well recognised and avoided, however the credential misuse has the highest anticipated value mostly due to the highest level of intention to perform such threat-posing actions (and omissions).

4. Practical implications

One of the practical implications of our article is to identify the various determinants of cyber-risky behaviour that may be measured. Shedding more light on this aspect can contribute to the creation of more tailored security policies in organizations, which can increase the cyber resilience of companies.

In our study, we uncovered the *environmental*, *credentials* and *behavioural* threats for which it is possible to measure factors related to an organisation's cyber resilience. The scale makes it possible to perceive the extent to which employees' intentions in each of the identified categories can increase or decrease cyber security. Intentions are often considered to be strong predictors of behavior as they take into account an individual's attitudes and beliefs, and intentions reflect an individual's motivation to engage in a particular behavior.

Considering the practical implications, they contribute to building an organisational culture focused on a good, positive approach to cybersecurity, which may take time but will ultimately protect companies from online threats in the long run. Organizations can strive to make good habits second nature to their employees, which in turn will help prevent hackers from exploiting existing security environments more effectively. In particular, rather than focusing on malicious

attacks, security policies should recognise that many breaches by employees are the result of trying to balance security and productivity.

5. Conclusions

The scale used for the study was updated with the actual exposure of employees to cyberthreats, and the research itself was conducted during the digital transformation of companies forced by the COVID-19 pandemic. Most previous studies employed separate scales to measure behaviour and attitudes, while the present study suggests a synergy of both approaches and the creation of a universal tool for analysing threat perception, behavioural tendencies and the aggregation of both of the above. Furthermore, the proposed research is supported by its immersion in the current reality created by the COVD-19 pandemic and associated changes in distributed workplaces, as well as the accelerated digital transformation of many organizations. Studies 1-3 achieved two basic objectives: (1) validating the scale of dangerous behaviour; (2) identifying three types of risk factors.

The results presented are a step towards understanding the differences in the behaviour and attitudes of employees, especially those working remotely, that can determine good cybersecurity practices, and underline the demand to focus directly on more effective training and awareness-raising mechanisms, which will result in companies being more resistant to cyber threats. The appropriate adaptation of measures to increase cybersecurity in the company will allow (1) its more effective operation and (2) reduced costs.

References

1. Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology, 33(3),* 237-248. doi: 10.1080/0144929X.2012.708787
2. Ajzen, I. (2011). The theory of planned behaviour: Reactions and reflections. *Psychology & Health, 26(9),* 1113-1127. doi: 10.1080/08870446.2011.613995
3. Ajzen, I., Fishbein, M. (1977). Attitude-behavior relations: A theoretical analysis and review of empirical research. *Psychological Bulletin, 84(5),* 888. doi: 10.1037/0033-2909.84.5.888
4. Alahmari, A., Duncan, B. (2020, June). *Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence*. 2020 international

conference on cyber situational awareness, data analytics and assessment (CyberSA). IEEE, pp. 1-5. doi: 10.1109/cybersa49311.2020.9139638

5. Anwar, M., He, W., Yuan, X. (2016, November). *Employment status and cybersecurity behaviors*. 2016 International Conference on Behavioral, Economic and Socio-cultural Computing (BESC). IEEE, pp. 1-2. doi: 10.1109/besc.2016.7804493
6. Anwar, M., He, W., Ash, I., Yuan, X., Li, L., Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69,* 437-443. doi: 10.1016/j.chb.2016.12.040
7. Arend, I., Shabtai, A., Idan, T., Keinan, R., Bereby-Meyer, Y. (2020). Passive-and not active-risk tendencies predict cyber security behavior. *Computers & Security, 97,* 101964. doi: 10.1016/j.cose.2020.101964
8. Bada, M., Sasse, A.M., Nurse, J.R. (2019). *Cyber security awareness campaigns: Why do they fail to change behaviour?* arXiv preprint arXiv:1901.02672. doi.org:10.48550/arXiv.1901.02672
9. Bada, M., Nurse, J.R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security, 27(3),* 393-410. doi: 10.1108/ics-07-2018-0080
10. Donalds, C., Osei-Bryson, K.M. (2020). Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents. *International Journal of Information Management, 51,* 102056. doi: 10.1016/j.ijinfomgt.2019.102056
11. Egelman, S., Peer, E. (2015, April). *Scaling the security wall: Developing a security behavior intentions scale (sebis).* Proceedings of the 33rd annual ACM conference on human factors in computing systems, pp. 2873-2882. doi: 10.1145/2702123.2702249
12. Enescu, S. (2019, June). *The concept of cybersecurity culture*. The Fourth Annual Conference of the National Defence College Romania in the New International Security Dynamics. Carol I National Defence University Publishing House, pp. 176-191. ISSN: 2668-3865
13. Ergen, A., Ünal, A.N., Saygili, M.S. (2021). Is It Possible to Change the Cyber Security Behaviours of Employees? Barriers and Promoters. *Academic Journal of Interdisciplinary Studies, 10(4),* 210. doi: 10.36941/ajis-2021-0111
14. Fishbein, M.E. (1967). *Readings in attitude theory and measurement*.
15. Gratian, M., Bandi, S., Cukier, M., Dykstra, J., Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security, 73,* 345-358. doi: 10.2307/588703
16. Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3(7), e00346*. doi: 10.1016/j.heliyon.2017.e00346

17. Hadlington, L.J. (2018). *Employees attitudes towards cyber security and risky online behaviours: an empirical assessment in the United Kingdom*. doi: 10.1016/j.heliyon. 2017.e00346
18. Hong, W.C.H., Chi, C., Liu, J., Zhang, Y., Lei, V.N.L., Xu, X. (2023). The influence of social education level on cybersecurity awareness and behaviour: A comparative study of university students and working graduates. *Education and Information Technologies, 28(1),* 439-470. doi: 10.1007/s10639-022-11121-5
19. Kumar, S., Yukita, A.L.K. (2021, May). *Millennials Behavioral Intention in Using Mobile Banking: Integrating Perceived Risk and Trust into TAM (A Survey in Jawa Barat).* International Conference on Business and Engineering Management (ICONBEM 2021). Atlantis Press, pp. 210-217. doi: 0.2991/aebmr.k.210522.028
20. Lu, S., Ye, J., Tan, Y. (2023, April). *Research on the Security of Data Cross-border Circulation in Cyberspace.* 2023 International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE). IEEE, pp. 1-8. doi: 10.1109/ICDCECE57866.2023.10151374
21. McBride, M., Carter, L., Warkentin, M. (2012). Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. *RTI International-Institute for Homeland Security Solutions, 5(1),* 1.
22. McCormac, A., Calic, D., Butavicius, M., Parsons, K., Zwaans, T., Pattinson, M. (2017). A reliable measure of information security awareness and the identification of bias in responses. *Australasian Journal of Information Systems, 21*. doi: 10.3127/ajis.v21i0.1697
23. McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior, 69,* 151-156. doi: 10.1016/j.chb.2016.11.065
24. McKinsey (n.d.). *How COVID-19 study has pushed companies over the technology tipping point and transformed business forever*. Retrieved from: https://www.mckinsey.com/ business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever, 30 June 2023.
25. Merhi, M., Hone, K., Tarhini, A., Ameen, N. (2021). An empirical examination of the moderating role of age and gender in consumer mobile banking use: a cross-national, quantitative study. *Journal of Enterprise Information Management, 34(4),* 1144-1168. doi: 10.1108/jeim-03-2020-0092
26. Monfared, A.R.K., Barootkoob, M., Sabokro, M., Keshavarz, M., Malmiri, M.M. (2023). The online stickiness circumstances in electronic retailing: website quality, perceived risk, and perceived value. *International Journal of Electronic Business, 18(1),* 51-76. doi: 10.1504/IJEB.2023.127532

27. Moustafa, A.A., Bello, A., Maurushat, A. (2021). The role of user behaviour in improving cyber security management. *Frontiers in Psychology, 12,* 561011.doi: 10.3389/fpsyg.2021.561011
28. Panko, R.R. (2010). *Corporate computer and network security*. Pearson Education India. doi: 10.3389/fpsyg.2021.561011
29. Pratama, A.R.I., Alshaikh, M., Alharbi, T. (2023). *Increasing cybersecurity awareness through situated e-learning: a survey experiment.* SSRN 4320165. doi: 10.2139/ssrn.4320165
30. Sağlam, R.B., Miller, V., Franqueira, V.N. (2023). *A Systematic Literature Review on Cyber Security Education for Children.* IEEE Transactions on Education. doi: 10.1109/TE.2022.3231019
31. Shropshire, J., Warkentin, M., Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security, 49,* 177-191. doi: 10.1016/j.cose.2015.01.002
32. Shropshire, J., Warkentin, M., Johnston, A., Schmidt, M. (2006). Personality and IT security: An application of the five-factor model. *AMCIS 2006 Proceedings, 415*. doi: 10.1016/j.cose.2015.01.002
33. Singer, P.W., Friedman, A. (2014). *Cybersecurity: What everyone needs to know*. OUP USA. ISBN: 978-0-19-991809-6
34. Uebelacker, S., Quiel, S. (2014, July). *The social engineering personality framework. 2014 Workshop on Socio-Technical Aspects in Security and Trust.* IEEE, pp. 24-30. doi: 10.1109/stast.2014.12
35. Ünal, A.N. (2020). What's Happenning in Cyber Space? An interdisciplinary approach. In: H.N. Keleş, A. Ergen (Eds.), *Cyberspace and Chaos: A Conceptual Approach to Cyber Terrorism* (pp. 103-126). Berlin: Peter Lang GmbH. doi: 10.3726/b16722
36. von Solms, B., von Solms, R. (2018). Cybersecurity and information security–what goes where? *Information & Computer Security, 26(1),* 2-9. doi: 10.1108/ics-04-2017-0025
37. Vroom, V.H. (1964). *Work and motivation*. NY: John Wiley &sons, 45. ISBN 0-471-91205-0
38. Wolfson, N. (1986). Research methodology and the question of validity. *TESOL Quarterly, 20(4),* 689-699. doi: 10.2307/3586519
39. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., Basim, H.N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems, 62(1),* 82-97. doi: 10.1080/08874417.2020.1712269

Appendix 1

Literature review

Limitation	No. of sources:
All fields with cybersecurity.	12,164
Only articles.	5,718
Category (Computer Science, Information Systems, Social Science, Business, Education, Behavioural Sciences, Sociology Sciences).	2,256
Titles review (we rejected articles describing cybersecurity models& frameworks, legal acts, regulations, technology applications, focus on threats and its nature).	1,182
Based on a review of titles supported by a review of abstracts in justified cases we selected a body of articles on cybersecurity and people, behaviour, employees and scales.	368
Based on the abstracts review, we selected the articles for literature review.	182

Appendix 2

Screen plot