Human TECHNOLOGY

ISSN: 1795-6889

https://ht.csr-pub.eu Volume 19(2), September 2023, 178–206

DO IT USERS BEHAVE RESPONSIBLY IN TERMS OF CYBERCRIME PROTECTION?

Hanna Yarovenko
Madrid University of Carlos III
Spain
Sumy State University
Ukraine
ORCID 0000-0002-8760-6835

Serhiy Lyeonov
University of Social Sciences
Poland
ORCID 0000-0001-5639-3008

Krzysztof Andrzej Wojcieszek
Academy of Justice,
Warsaw, Poland
ORCID 0000-0003-1047-8000

Zoltán Szira
Budapest Metropolitan University,
Budapest, Hungary
ORCID 0000-0002-7299-4695

Abstract: *This study aims to analyze the behaviour of IT users regarding their personal protection against potential cybercrimes. The research data set is based on surveys conducted by the European Commission in 2020-2021 for 35 European countries. Canonical analysis revealed that 66.67% of cybercrime cases (Phishing, Pharming, Online identity theft, etc.) determine individuals' choice of personal protection method (using a security token, social media logins, electronic identification, etc.). Kohonen's self-organizing maps were used to form 9 clusters of countries depending on the attitude of IT users to personal cybersecurity. The map results showed that individuals behave less responsibly using a security token, electronic identification certificate or card, pin code list or random characters of a password, and other electronic identification procedures. Users from Denmark, the Netherlands, Iceland, Norway, the UK, Austria, and Finland were the most responsible Europeans in terms of personal protection, while people from Bulgaria, Romania, Serbia, Albania, North Macedonia, Bosnia and Herzegovina were the least conscientious about protection.*

Keywords: *cybercrime, IT user, Kohonen map, personal cybersecurity, responsible behaviour, protection.*

DOI: https://doi.org/10.14254/1795-6889.2023.19-2.3

INTRODUCTION

The consequences of Industry 4.0 and the beginning of its new 5.0 phase have been influencing the development of social life. Although the Fourth Revolution was focused on automating many processes and simplifying their execution by a person, the next stage aims to achieve a balanced interaction between humans and computer technologies based on artificial intelligence and intricate robotic complexes. On the one hand, these processes positively impact society, the economy, and the environment and ensure sustainable development. On the other hand, rapid digitization and automation have given rise to new types of crime. Cybercrimes are illicit actions conducted by a person or a group of persons aimed at individual users, companies, governments, and even countries that use information and communication technologies. They result in theft or leakage of personal data, especially financial data, malfunctioning of mobile devices, computers, enterprise infrastructure, damage to software, etc.

Statistics show that the level of cybercrime in the world is constantly increasing. In 2001, six people per hour became victims of cybercrimes. In 2022, this number increased almost 15 times to 91 people, although the maximum number reached 97 victims per hour in 2021 (Surfshark, 2022). Comparitech research team estimated that approximately 71.1 million people suffered from cybercrime annually (Bischoff, 2022). Every ten-thousandth resident of the European Union became a victim of cybercrime in 2020 (Vasilyeva et al., 2022). A 2007 University of Maryland study found that a cyber hacker attack occurred every 39 seconds (Cukier, 2007). However, according to the Internet Crime Complaint Center of the Federal Bureau of Investigation, one successful attack occurred every 1.12 seconds in 2020 (Federal Bureau of Investigation, 2020). This indicates that the frequency and effectiveness of cybercrime is increasing. If cybercrime financial losses per hour in 2001 amounted to $2,055, this figure increased approximately 572 times by 2022 and amounted to $1,175,799 (Surfshark, 2022). According to expert estimates, losses from cybercrime in 2018 reached 0.86 trillion U.S. dollars; by 2022, they increased 9.8 times and equalled 8.44 trillion U.S. dollars. In 2027, they may increase to 23.82 trillion U.S. dollars (Fleck, 2022).

The given data show that cybercrime has become a serious problem for ensuring the sustainable development of society. At the same time, it has a peculiar, steady growth trend, facilitated by a significant decrease in the price of computer technologies and an increase in their availability for ordinary IT users. For example, the IT market offers cybercrime devices that start at $1, making it easy for anyone to become a cybercriminal (Rapp & Hackett, 2017). It is not for nothing that the World Economic Forum (2022) singles out the spread of cybercrime among the ten most critical risks for the world. Thus, in ranking risks that have worsened since the beginning of the COVID-19 pandemic, cybersecurity mistakes leading to the spread of cybercrimes occupy the seventh position. Among the risks that will become the most serious threat worldwide in the next two years, it also ranks seventh, and among those that will be critical in the next five years, it ranks eighth. That is why combating cybercrimes is the prerogative of the cyber defense department. However, 88% of cybersecurity breaches are caused by human factors, and since anti-virus software is only 50% effective, the IT user's behavior influences the success or failure of cyber attacks (MacKay, 2022). According to a survey conducted by KPMG, 86% of respondents believe that it is IT users who are responsible for data security. However, 90% identify the responsibility as government and 91% as business

(Orson & Stein, 2020). It follows from this that an individual's behavior in cyberspace is important in the personal security organization, forming his/her security environment.

What is responsible behaviour, and why is it so important today? It is a key issue surveyed by the Geneva Dialogue on Responsible Behavior in Cyberspace. This project was launched in 2018 by the Swiss Federal Department of Foreign Affairs (FDFA), the Geneva Internet Platform (GIP), the United Nations Institute for Disarmament Research (UNIDIR), ETH Zurich and the University of Lausanne. The main goal was to identify the stakeholders - the state, business entities and civil society - and their roles in using information and communication technologies for security in global cyberspace. Within the framework of the organized webinar "What is responsible behaviour in cyberspace?" it was determined that responsible behaviour is "behaviour by a given actor in a given set of circumstances that can be said to conform to the laws, customs and norms generally expected from that actor in those circumstances" (Gavrilović, 2018). This concept does not fully reveal its essence and needs to be clarified depending on the roles that various subjects perform in cyberspace. It especially applies to the determination of the individual IT users' behaviour, which should be based on their attitude to protecting personal data and applying basic and particular actions to counter cyber threats. For example, ignoring emails received in spam or from unfamiliar addresses, regularly changing passwords, not disclosing personal, especially financial, information in social networks, etc.

The Geneva Dialogue has proposed and implemented many initiatives related to the responsible behaviour of states in cyberspace. 11 central voluntary UN norms define what states can and cannot do as part of their responsible behaviour in cyberspace (Hogeveen, 2022). However, to a greater extent, this activity is directed at the macro and global level of cyberspace. As for ordinary IT users, a mechanism for increasing digital literacy on personal security issues is proposed. Since it is very difficult to regulate the cyber protection of every citizen at the state or global level, the spread of educational activities should deepen individuals' awareness in this area and motivate them to apply more advanced security measures.

Based on the above, should society combat cyber threats? Sure, because the losses from cybercrimes can be quite tangible for their victims. Who should be responsible for personal safety? In most cases, each IT user should be responsible for personal cyber protection, but this should also not abdicate the responsibility of companies, governments and international organizations. How should an IT user behave in such cases? His/her behaviour must be responsible, including applying a set of actions aimed at protecting personal data. Is this how IT users behave today? This study will deal with the answers to this question.

LITERATURE REVIEW

Today, digitization and computerization processes are important factors in achieving the benefits of the economy and sustainable development of the country for the long term (Tiutiunyk et al., 2021; Millia et al., 2022). Thanks to them, the processes of convergence of the cybersecurity system with the economy and business take place (Kuzior et al., 2022). For example, some Internet users directly affect economic growth, especially in transition

economies (Remeikiene et al., 2021). Mobile technologies contribute to increasing the level of human well-being (Rosenberg & Taipale, 2022).

The scope of application of modern information and communication technologies is broad. Their features have been studied and continue to be studied for health care (Alimbaev et al., 2021), construction (Popov et al., 2021), transport (Okunevičiūtė Neverauskienė et al., 2021), finance (Mnohoghitnei et al., 2022) and the banking sector (Haddad, 2021), the hospitality and tourism industry (Lustigova et al., 2021), small and medium-sized businesses (León-Gómez et al., 2022), e-commerce (Kiba-Janiak et al., 2022), e-government (Kolosok et al., 2022). Despite the field of activity, global, macro-, micro- or individual level, the key figure is always the person who plays an important role in the digital transformation processes (Tran et al., 2022). Therefore, the effectiveness of the information and communication technologies will depend on its behaviour, which will affect the cybersecurity level, both personal and for enterprises, the country and the world as a whole.

Where is the individual's responsible behavior most important to ensure cybersecurity? The current development of technologies is aimed at their evolution from being used in simple calculations to playing the key role of a decision-maker in a company (Gladden et al., 2022). Therefore, today, humanity wants to consolidate the role of the host in its interaction with artificial intelligence technologies (Tugui et al., 2022). Beňo (2022) proved the existence of a direct correlation between the number of highly educated and electronic workers, indicating the intellectualization of work that requires the IT application. On the one hand, it contributes to developing cybersecurity measures. On the other hand, it can lead to the future degeneration of many professions since introducing technological innovations always leads to increased unemployment (Lydeka & Karaliute, 2021). Some individuals have difficulty integrating into digital technologies, such as the oldest generation and members of the younger generation (Dečman et al., 2022). That is why they often become victims of cybercrimes because they do not have enough knowledge to apply basic protection tools. However, the advantages of society digitalization allow the use of electronic learning tools that help to increase the level of digital and cyber literacy of users regardless of age, status, and type of activity (Davidovitch & Eckhaus, 2022).

The global pandemic of COVID-19 contributed to the fact that most companies transferred employees to remote work. On the one hand, it should have contributed to a significant reduction in costs, but this factor may not be confirmed in practice (Navickas et al., 2022). On the other hand, it led to the appearance of vulnerabilities in the cyber defence system due to the influence of the human factor (Kobis & Karyy, 2021). In such cases, it is reasonable to create virtual teams, which contribute to the development of human capital, ensure the organizational sustainability of enterprises and can contribute to increasing the effectiveness of cybersecurity measures (Capolupo et al., 2022). The experience of using virtual reality in tourism confirms it (Florek & Lewicki, 2022). The information technology factor is not influential for knowledge management in enterprises (Gad & Yousif, 2021). However, the exchange of knowledge between company employees can affect the quality of information systems of companies, forming the appropriate knowledge banks for countering cybercrimes (Zamir & Kim, 2022).

The vulnerability of IT users' cybersecurity is noticeable in the electronic services of the financial sphere. For example, electronic banking is firmly rooted among them and is the most used by individuals. Their quality in general and security in particular directly impact the satisfaction and loyalty of electronic customers of banks (Ahmed et al., 2021). Hassan & Lee

(2021) prove that a key factor in the perception of e-commerce is consumers' level of trust in this type of service, which can undoubtedly influence the personal cybersecurity measures they use in online payments. Fülöp et al. (2022) found a positive impact of Fintech Accounting and Industry 4.0 technology on increasing trust in digital accounting services. Blockchain technologies and smart contracts increase the reliability of partners and contribute to the competitiveness of enterprises, although they can act as a source of information vulnerability for cybercriminals (Chen et al., 2022).

Speaking about information technologies and their impact on society, business, and individuals, one should remember the ethics of this issue (Constantinescu & Edu, 2022). It is because disclosing personal data online can become a vulnerable link and create favourable conditions for cybercriminals. Therefore, companies and governments should pay attention to implementing tools that ensure this issue's ethical side.

The possibilities of information and communication technologies are powerful. The introduction of artificial intelligence, industrial robots, blockchains, smart contracts, smart cities, etc., makes life easier and contributes to the country's economic development. At the same time, they create opportunities for cybercriminals. Therefore, the level of cybersecurity will depend on the company employees' behaviour, as well as users of relevant services and technologies. It includes digital literacy, quality of services, intellectualization and virtualization of work, knowledge exchange, cyber ethics, etc.

METHODS AND DATA

Data

The article used data from surveys conducted by the European Commission in 2020-2021 for 35 European countries. Two sets of data were used in the study. The first set includes eight indicators characterizing the number of respondents who have encountered cybercrime cases (Eurostat, 2022c). The second set concerns the interviewees' answers regarding appropriate measures of personal cyber protection.

The first data set identifies the relationship between cybercrime incidents and responsible behaviour. It included an indicator "Fraudulent credit or debit card use" showing what percentage of respondents had fallen victim to fraudulent credit or debit card use. This type of cybercrime is social engineering, which assumes that a fraudster misleads a person and voluntarily gives information related to his/her bank cards. A second indicator "Online identity theft" is the number of individuals who have had their personal information stolen online, allowing the criminal to impersonate the victim and gain some benefit. A third indicator "Phishing" shows the number of respondents who became phishing victims, i.e., received fraudulent messages from cybercriminals. A fourth indicator "Pharming" is the number of victims of pharming, i.e., they were redirected to fake websites that asked for personal information. The fifth indicator "Misuse of personal information available on the Internet" is the number of respondents who experienced abuse of their personal information online, resulting in discrimination, harassment or bullying by cybercriminals. The sixth indicator "Social network or e-mail account being hacked" is the number of victims of social network or email account hacking, as well as posting or sending content without the knowledge of

individuals. The seventh indicator "Data loss due to a virus" is the number of individuals who lost personal information (documents, videos, images, etc.) due to a virus attack and infection of a computer or other device. The final indicator "Identity theft, receiving fraudulent messages or being redirected to fake websites" is the percentage of respondents who experienced financial loss as a result of having their personal information stolen, receiving fraudulent messages, or being redirected to fake websites.

The second data set includes 16 indicators reflecting the percentage of individuals who demonstrate behaviour in the information environment in the form of their implementation of specific cyber protection actions. These are the following indexes: "Using simple login with username and password", "Using a social media login", "Using a security token", "Using an electronic identification certificate or card with a card reader or an app", "Using a procedure involving the mobile phone", "Using a single-use PIN code list or random characters of a password", "Using other electronic identification procedures", "Using at least 4 identification procedures", "Individuals know that cookies can be used to trace the movements of people on the Internet", "Changing the settings in the internet browser to prevent or limit cookies on any devices", "Using software that limits the ability to track activities on the Internet", "Reading privacy policy statements before providing personal data", "Restricting or refusing access to the geographical location", "Limiting access to profiles or content on social networking sites or shared online storage", "Rejection of using personal data for advertising purposes", "Checking the security of the website where personal data is provided". The data from the first to the eighth indicator were taken from the results of the survey conducted by Eurostat (2022a), and from the ninth to the sixteenth, from Eurostat (2022b).

Methods

Several stages are foreseen in the study. In the first stage, linear dependencies are studied, and the relationships between two sets of variables are identified. One of them is formed by variables characterizing the number of respondents who have encountered cybercrime cases. The second is represented by indicators that determine the responsible behaviour of IT users. For this stage, canonical analysis is used to assess the influence of one set on another and substantiate its statistical significance. The canonical analysis will reveal a group of factors and individual factors of greatest influence. The statistical significance of the correlation between groups of indicators and the statistical significance of canonical roots will be checked using the χ^2 distribution. The calculated value χ^2 is compared to the critical one. If it is smaller, the value of the correlation between groups of indicators is statistically significant. At the same time, the p-value is also estimated, which should not exceed 0.05, confirming statistical significance.

In the second step, data standardization and assessment of the multicollinearity of the data array is carried out. Standardization will help scale the data to the value of the variance and cancel out the effect of the averages. For this purpose, Z-score normalization is used (Kreyszig, 1979). For checking the array of data for the presence or absence of multicollinearity, $\chi^2$is used which will be calculated based on the data of the entire array. The obtained value is compared with the critical value if $\frac{1}{2}m(m-1)$ – freedom degrees and the corresponding level of significance α. If $\chi^2 > \chi^2_{cr}$, there is multicollinearity in the array of variables, otherwise it is absent.

In the third step, the principal component method is used to reduce the dimensionality of the data and eliminate multicollinearity. This procedure will help to avoid the influence of this phenomenon when justifying the number of clusters.

In the fourth step of the research, the number of clusters is substantiated using the Silhouette technique. Most researchers use the Elbow method to perform this task, but it only calculates the Euclidean distance. The Silhouette method considers various features - dispersion, asymmetry, the difference between maximum and minimum values, etc. This method was proposed by Rousseeuw (1987) to check the consistency of data in clusters using visualization. Its main purpose is to calculate the silhouette coefficient for all observations of the sample and for the cluster as a whole, taking into account the average distance between the group and the average distance to the nearest cluster. Silhouette scores are calculated according to formula (1) (Rousseeuw, 1987):

$$\begin{cases} s(i) = \dfrac{k(i) - l(i)}{max\{k(i), l(i)\}}, if\ |O_I| > 1, \\ s(i) = 0, if\ |O_I| = 1 \end{cases} \quad (1)$$

where $s(i)$ is a silhouette score for i-th observation from the data sampling; $k(i)$ is the average distance between i-th observations and other cluster observations; $l(i)$ is the shortest distance between i-th observations in the cluster to other observations of other clusters; $|O_I|$ is a set of observations of one cluster. Accordingly, the average and shortest distances are calculated using formulas (2) – (3) (Rousseeuw, 1987):

$$k(i) = \frac{1}{|O_I| - 1} \sum_{j \in O_I, i \neq j} d(i,j), \quad (2)$$

$$l(i) = \min_{J \neq I} \frac{1}{|O_J|} \sum_{j \in O_J} d(i,j), \quad (3)$$

where $d(i,j)$ is the distance between i-th and j-th observations.

Since the Silhouette score is used to justify the number of clusters in this methodology, the corresponding scores will be calculated for their different number. To make a decision, it is necessary that $s(i) \to 1$. The estimate close to one indicates that the distribution of observations on a given number of clusters is the most effective.

In the fifth step, self-organizing Kohonen maps, a technique of unsupervised machine learning allowing to create a two-dimensional data representation in the form of maps while preserving the data structure, are built. Maps are formed from neurons or nodes associated with a vector of weight estimates determining their position in space. The learning process consists of moving the weight estimates in such a way as to reduce the distance between neurons. First, the input vector of weights is chosen randomly. Then, there is a transition from neuron to neuron. This process is accompanied by determining the similarity of the input vector and the vector of weight estimates corresponding to a node on the map. The neuron with the smallest Euclidean distance value is assigned the matching unit. Based on this knowledge, the weight

vectors of neurons are updated in combination with the best matching unit (formula (4), Kohonen & Honkela, 2007):

$$W_v(r+1) = W_v(r) + \theta(u, v, r) \cdot \alpha(r) \cdot (B(t) - W_v(r)), \quad (4)$$

where $W_v(r+1)$ is the updated vector of weights of the neuron taking into account r– iterations of updating the weights; W_v is the current vector of neuron weights; $\theta(u, v, r)$ is a neighborhood function that defines the distance between two neurons – u and v on the step r; u is the index of the best matching neuron score in the map; v is the index of the neuron in the map; $\alpha(r)$ are limitations of the learning process or a monotonically decreasing learning coefficient; $B(t)$ is the vector of input weights.

After updating the weight vector, the iteration step r is increased. The procedure is repeated until it reaches the final limit of the iteration. As a result of applying the unsupervised machine learning technique, a Kohonen map is built, demonstrating the distribution of the analyzed elements according to the corresponding clusters. It helps to analyze the elements grouped according to the similarity of their characteristics.

RESEARCH RESULTS

At the first stage of the proposed methodology, a canonical analysis was performed between the two data sets using the STATISTICA analytical package. Figure 1 presents the obtained results.

N=35	Canonical Analysis Summary Canonical R: .95865 Chi²(128)=155.70 p=.04877 Left Set	Right Set
No. of variables	8	16
Variance extracted	100.000%	66.2904%
Total redundancy	66.7662%	48.9594%
Variables: 1	Fraudulent credit or debit card use	Using a simple login with username and password
2	Online identity theft	Using a social media login
3	Phishing	Using a security token
4	Pharming	Using an electronic identification certificate or car with a card reader or an app
5	Misuse of personal information available on the Internet	Using a procedure involving the mobile phone
6	Social network or e-mail account being hacked	Using a single -use PIN code list or random characters of a password
7	Data loss due to a virus	Using other electronic identification procedure s
8	Identity theft, receiving fraudulent messages or being redirected to fake websites	Using at least 4 identification procedures
9		Individuals know that cookies can be used to trace the movements of people on the Internet
10		Changing the settings in the internet browser to prevent or limit cookies on any devices
11		Using software that limits the ability to track the activities on the Internet
12		Reading privacy policy statements before providing personal data
13		Restricting or refusing access to the geographical location
14		Limiting access to profile s or content on social networking sites or shared online storage
15		Rejection of using personal data for advertising purposes
16		Checking the security of the website where personal data is provided

Figure 1. Results of the canonical analysis.
[Source: calculated by the authors]

Figure 1 shows a high value of the canonical correlation ($R = 0.95865$), indicating that there is a strong correlation between the set of selected cybercrime cases (Left Set) and indicators characterizing the responsible behaviour of IT users (Right Set). The statistical significance of the correlation coefficient is confirmed by the high value of the Pearson test ($\chi^2 = 155.70$), the significance level of which does not exceed 0.05 ($p = 0.04877$). The redundancy value for the left set is 66.7662%; i.e., the right set variables, which correspond to IT users' responsible behaviour indicators, explain 66.7662% of the changes caused by cybercrime cases. In two out of three cases, the user's vulnerability in the network depends on incorrectly or insufficiently correctly chosen personal cyber protection tools. In turn, the cases of cybercrimes explain by 48.9594% the variability of the IT users' behaviour regarding

personal cyber protection, i.e., in approximately 50% of cases, the choice of the appropriate person's behaviour regarding its protection depends on the type of cybercrime.

For further analysis, it is necessary to select those canonical roots that are statistically significant. The result of the obtained roots and verification of their statistical significance is presented in Figure 2.

	Chi-Square Tests with Successive Roots Removed					
Root Removed	Canonicl R	Canonicl R-sqr.	Chi-sqr.	df	p	Lambda Prime
0	0.9586455	0.9190012	155.6953	128	0.048774	0.0007161
1	0.9013787	0.8124835	101.6590	105	0.574071	0.0088413
2	0.8012128	0.6419420	65.6704	84	0.930365	0.0471494
3	0.7208380	0.5196074	43.5886	65	0.980964	0.1316808
4	0.6607936	0.4366482	27.8258	48	0.991270	0.2741108
5	0.5692695	0.3240677	15.4880	33	0.995882	0.4865712
6	0.4537064	0.2058495	7.0673	20	0.996454	0.7198520
7	0.3058713	0.0935572	2.1119	9	0.989569	0.9064428

Figure 2. Evaluation of statistical significance of canonical roots.
[Source: calculated by the authors]

Figure 2 shows that the Chi-square in the first row, corresponding to the analysis without root removal, is statistically significant because $p < 0.05$, so, at least one canonical root is also statistically significant. When it was removed, the authors found that the remaining roots were statistically insignificant. Therefore, the result is one statistically significant root, i.e., it is appropriate to consider one pair of canonical variables. To confirm these conclusions, the authors demonstrate the factor structure and redundancy (Appendix A, Figures 1-2).

The largest factor loadings have indicators to the first root, both for the left and right set, confirming the previous conclusion. Since the factor loadings represent correlations between the set indicators, the responsible IT users' behaviour indicators demonstrate average, above-average and significant correlations. Only the variable related to "Reading privacy policy statements before providing personal data" shows a very weak relationship, which indicates the insignificance of this responsible behaviour type for countering cybercrimes (Appendix A, Figure 1, Row 12). "Using at least 4 identification procedures" and "Using a procedure involving the mobile phone" is the most correlated (Appendix A, Figure 1, Rows 5 and 8). Users who apply multiple cyber protection tools are more likely to use a mobile phone to confirm their actions on the Internet. These measures are the factors reducing the vulnerabilities of users' security and affecting the number of cybercrime cases.

The least correlated cybercrime cases are those related to losing personal information due to a virus attack (Appendix A, Figure 2, Row 7). The highest level of communication is demonstrated by "*Fraudulent credit or debit card use*" and "*Identity theft, receiving fraudulent messages or being redirected to fake websites*" (Appendix A, Figure 2, Rows 1 and 8). It suggests that IT users who were victims of fraudulent use of credit or debit cards may also have experienced identity theft. At the same time, phishing cases have a weak connection with other cases of cybercrime.

Canonical weights were determined to understand which responsible behavior measures and cybersecurity cases are the most important (Appendix A, Figures 3-4). The value of

canonical weights, taken by the module, determines the contribution of each indicator to the formation of canonical variables. The greatest contribution to the responsible behaviour of IT users will be made by "Using at least 4 identification procedures" (|0.397156|), "Using a procedure involving the mobile phone" (|0.360203|), "Restricting or refusing access to the geographical location" (|0.351491|), "Limiting access to profiles or content on social networking sites or shared online storage" (|-0.2732531|), "Checking the security of the website where personal data is provided" (|-0.2598138|), "Individuals know that cookies can be used to trace the movements of people on the Internet" (|0.2342221|) (Appendix A, Figure 3). "Using other electronic identification procedures" (|-0.004255596|), "Using a single-use PIN code list or random characters of a password" (|0.008669309|), "Using software that limits the ability to track the activities on the Internet" (|-0.01907673|), "Using an electronic identification certificate or card with a card reader or an app" (|-0.041001|), "Using a simple login with username and password" (|0.06513116|), "Rejection of using personal data for advertising purposes" (|0.04041022|). Positive variables indicate that increasing these measures will effectively increase the cases where IT users become victims of the respective cyber threats (Appendix A, Figure 3). Negative values indicate a decrease in the effectiveness of applying these measures under such conditions.

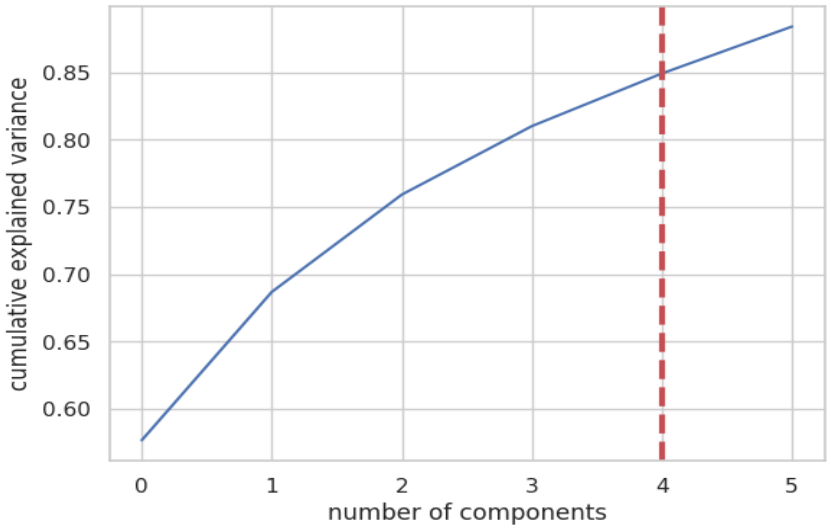
All values are significant when it comes to cybercrime cases. The biggest contribution will be made (Appendix A, Figure 4) by "Misuse of personal information available on the Internet" (|0.6336418|), "Online identity theft" (|-0.4745117|), "Fraudulent credit or debit card use" (|0.374483|), "Data loss due to a virus" (|-0.3130664|), "Identity theft, receiving fraudulent messages or being redirected to fake websites" (|0.2306303|). These variables will strongly influence the responsible behaviour of IT users. Positive values indicate that as cybercrime cases increase, the number of users applying personal security measures will increase. The negative values show feedback. The growth of such cybercrimes affects the decrease in IT users who will install appropriate security measures. It occurs because the security measures in this study that shape the individuals' responsible behaviour are not effective enough to counter these cyber threats.

The next part of the study defines clusters of countries where the respondents are more or less responsible for personal protection. For this purpose, it was determined whether multicollinearity exists in the array of variables. The calculated value of the determinant of the correlation matrix is equal to 3.8493E-09. Its value approaches zero, i.e., there is multicollinearity between the explanatory variables. Accordingly, the calculated value of the Chi-sqr criterion is equal to $\chi^2 = 539.2813$ and exceeds its critical level ($\chi^2{}_{cr} = 146.5674$), defined for $0.5m(m-1)$ freedom degrees and significance level $\alpha = 0.05$. It confirms the multicollinearity in the array of variables.

For ist eliminating and reducing the data dimensionality, the principal component method performed using Python programming was applied. Its results are presented in Figure 3, where it can be seen that the first component explains 57.6619% of the total variation, the second – 11.0215%, the third – 7.2305%, and the fourth – 5.0867%. The other components explain less than 5% of the total variation each. Therefore, the authors decide that the first four components should be chosen for further calculations and justification of clusters, which together explain 81.0006%.

Silhouette Scores were used to determine the potential number of clusters (Figure 4). The results show that the most similar objects correspond to 11 clusters. Since the studied data set

contains observations for 35 countries, using many groups contributed to obtaining those with only one country. Therefore, it was decided to form 9 clusters since this value corresponds to the next highest Silhouette Score. Later, this distribution turned out to be optimal, confirmed by the analysis of average values for each cluster.



	Cumulative Variance Ratio	Explained Variance Ratio
0	0.576619	0.576619
1	0.686833	0.110215
2	0.759139	0.072305
3	0.810006	0.050867
4	0.849109	0.039103
5	0.883951	0.034842

Figure 3. The results of the principal component method.
[Source: calculated by the authors]

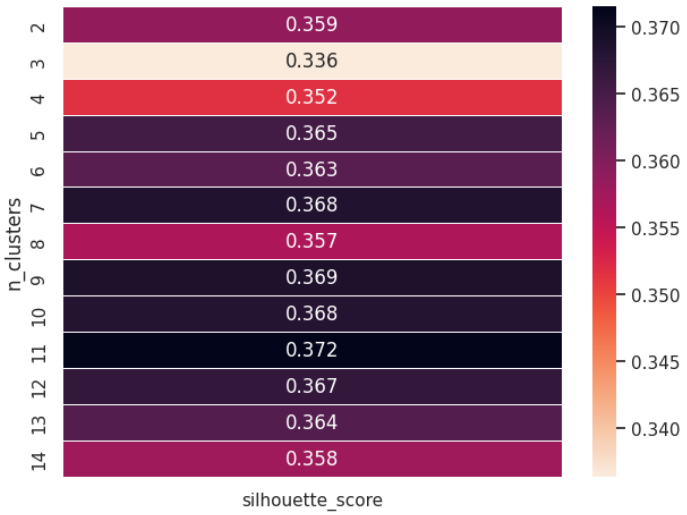


Figure 4. Results of cluster significance assessment using Silhouette Score.
[Source: calculated by the authors]

The Viscovery SOMine analytical package was used to obtain Kohonen maps. Under this process, various methods of its construction were experimentally tested. As a result, a map with 1000 nodes and an automatic ratio of 51:21 was trained. A Normal training schedule with a voltage of 0.5 and temperature of 0.2 was also used. The Ward (hierarchical) method with 9 clusters was chosen as an algorithm for initial clustering. The indicator weights, taken from the canonical analysis results, were set. Based on the given features, clusters of countries were obtained, grouped by the level of responsible behaviour of IT users towards personal cyber protection (Figure 5).

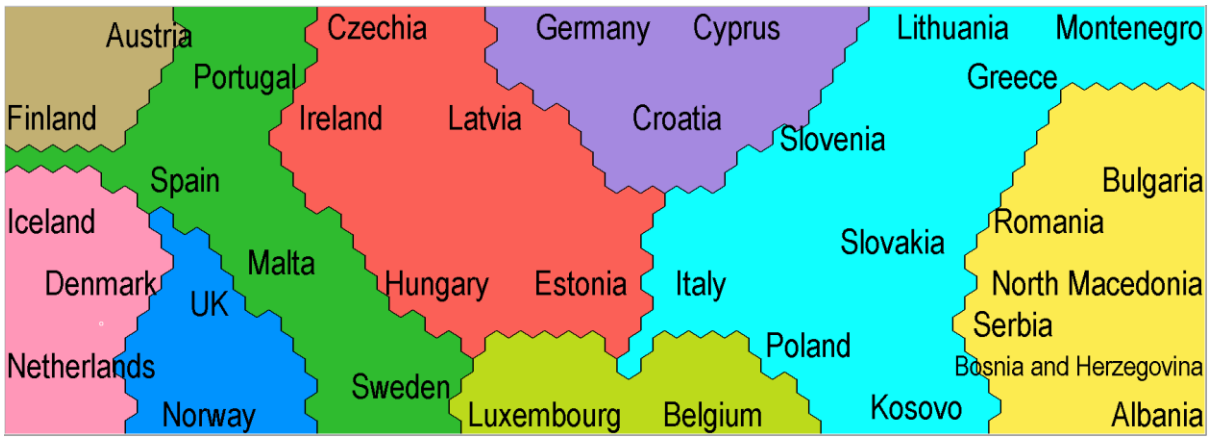


Figure 5. Map of Kohonen.
[Source: calculated by the authors]

The lowest level of responsible behaviour of IT users characterizes the clusters on the right in Figure 5. Thus, the third cluster (C3) includes six countries: Romania, Bulgaria, Serbia, Albania, North Macedonia and Bosnia and Herzegovina (Figure 5, yellow cluster). Analyzing the average values (Appendix B, Table 1), it can be concluded that this group has the lowest level of responsible behaviour of IT users. This means that the respondents from these countries

pay little attention to personal protection in carrying out activities using computers and mobile devices. The first largest cluster (C1) includes eight countries - Montenegro, Lithuania, Greece, Slovenia, Slovakia, Italy, Poland, and Kosovo (Figure 5, turquoise cluster). Their averages (Appendix B, Table 1) show that the number of respondents who used the analyzed personal security tools is more significant than for the third group, i.e., IT users are more responsible for their protection.

The share of respondents from the countries in the left clusters in Figure 5 is the highest, indicating their high level of responsibility for personal cybersecurity. So, cluster 6 (C6) includes three countries – Denmark, Iceland, and Netherlands (Figure 5, pink cluster), cluster 8 (C8) – United Kingdom and Norway (Figure 5, blue cluster), cluster 9 (C9) – Finland and Austria (Figure 5, brown cluster). Their average values (Appendix B, Table 1) for most indicators are the highest, confirming the conclusion about the high level of responsible behavior of IT users from these countries.

As for the other clusters, closer to the centre of Figure 5 (green cluster – C4, red cluster – C2, purple cluster – C5, olive cluster – C7), they are characterized by moderate behaviour of individuals regarding personal cyber protection. This conclusion is confirmed by the average values for each indicator under the created group (Appendix B, Table 1).

The authors analyze the Kohonen maps for each of the selected indicators. The map generated for "Using a simple login with username and password" (Appendix C, Figure 5a) shows an exemplary distribution by clusters. IT users from Norway, Great Britain, the Netherlands, Iceland, the Czech Republic and Germany prefer this tool. Respondents from the third cluster and Montenegro countries use this security measure less actively. Figure 5b in Appendix C shows the behaviour for "Using a social media login". According to this indicator, the distribution is uneven for some clusters. For example, in the first cluster, respondents from Kosovo preferred this protection method more than respondents from other countries. Users from Luxembourg and Belgium have diametrically different attitudes towards the use of this measure for working on the Internet.

The map showing the distribution of clusters according to the indicator "Using a security token" (Appendix C, Figure 5c) also has certain exceptions for Croatia, Luxembourg, Montenegro, Malta, etc. This type of cyber protection is most popular among IT users in Norway. It is the least popular for the third cluster countries. Such discrepancies indicate that this tool is quite specific, and perhaps not enough people are ready to use it for security purposes. Figure 5d of Appendix C shows the behaviour regarding using an electronic identification certificate or card with a card reader or an app. The results of distribution by clusters are also heterogeneous. It can be clearly observed in Iceland, Sweden, Estonia and Lithuania. Although this security measure is quite famous for calculation in various Internet services, for the respondents from most countries, there is no suitable application for personal protection.

The map created for "Using a procedure involving the mobile phone" (Appendix C, Figure 5e) shows a reasonably weighted distribution by clusters, clearly visible in the example of the sixth and eighth clusters countries, using this security measure the most. It is the least popular for residents of the third cluster. Figure 5f of Appendix C shows the behaviour for "Using a single-use PIN code list or random password characters". The colour gradation of the map indicates the uneven application of this measure for most clusters. Residents of Denmark and Finland give the greatest preference to its use. IT users in the vast majority of countries limit

the use of this security measure, possibly due to the difficulty to remember complex random passwords and the loss of further access to their account.

The map showing the distribution of clusters according to the indicator "Using other electronic identification procedures" (Appendix C, Figure 5g) shows some exceptions for the Netherlands, Spain, Denmark and Hungary. In general, a situation shows the unpopularity of other security measures. In most cases, IT users apply well-known traditional tools; a relatively low percentage try to use other additional ones. Figure 5h of Appendix C shows the behaviour of using at least four identification procedures. The colour distribution of the map indicates the uniformity of this security measure in the middle of individual clusters. At the same time, it is preferred by Iceland, the Netherlands, Denmark, Norway and Great Britain residents. The lowest level of responsibility in this case is demonstrated by IT users of countries belonging to the third cluster.

Figure 6a of Appendix C shows the behaviour of individuals who know that cookies can be used to trace people's online movements. The colour gradation of the map indicates a good balance of the distribution of values for most clusters. This type of behaviour is one of the popular activities among others. It is preferred by respondents from those countries that belong to high-responsibility clusters. It is the least popular among users of the third cluster. The map shows A fairly even distribution for the indicator "Changing the settings in the internet browser to prevent or limit cookies on any devices" (Appendix C, Figure 6b). But some clusters have intra-group differences, for example, fifth, seventh, sixth and ninth.

The map in Figure 6c of Appendix C shows the cluster distribution according to the "Using software that limits the ability to track the activities on the Internet" indicator. Generally, it shows a balanced formation of clusters, although there are exceptions for Belgium, Malta and Cyprus. At the same time, this tool is the most popular among individuals from Belgium and the least - from Cyprus. If we compare this measure with others, users give it a much lower preference than "Using a simple login with username and password", "Using a procedure involving the mobile phone," or "Individuals know that cookies can be used to trace the movements of people on the Internet". Figure 6d of Appendix C shows the distribution by group for "Reading privacy policy statements before providing personal data". Most respondents from Finland, Austria, Germany, and Cyprus chose this type of protection. Not preferred by IT users from Luxembourg, Belgium and Albania.

Figure 6e of Appendix C demonstrates the behaviour of individuals who restrict or refuse access to the geographical location. The colour gradation of the map shows a fairly even distribution of values for most clusters. This security measure is preferred by users of countries grouped into clusters with the highest responsibility. It is not famous for clusters with a low level of responsible behavior. The map in Figure 6f of Appendix C characterizes the distribution according to the indicator "Limiting access to profiles or content on social networking sites or shared online storage". Some clusters have within-group differences, such as the third, fourth, and ninth. In general, this security measure is quite popular among IT users of different countries.

The map in Figure 6g of Appendix C refers to the behaviour of individuals to reject of using personal data for advertising purposes. One should be noted the balanced distribution of countries by this type of personal cyber protection, but there are exceptions for Iceland, Kosovo and Latvia. This measure is famous for the countries of the left-hand cluster (Figure 5) and the Germany-Cyprus-Croatia sector. The countries of the third cluster do not prefer it. Figure 6g

of Appendix C demonstrates the behaviour of individuals who check the website's security where personal data is provided. IT users in the Netherlands apply this tool more often than others. Respondents from Albania prefer him less than individuals from other countries.

DISCUSSION

The issue of cybersecurity behaviour is an understudied area of research to date, as evidenced by Oliveira & Baldi (2022). But despite the limited information on this problem, Pollini et al. (2022) believe that human components of sociotechnical systems are its weakest and most vulnerable component. Therefore, their responsible behaviour in the computer environment affects the level of personal, corporate or state cybersecurity. This statement is synchronized with the obtained results of this article. Although there are many best practices today, IT users' application of the most effective security and privacy methods remains relatively low (Krsek et al., 2022).

People's awareness of cyber threats strongly influences proactive cybersecurity behaviour, especially after the global pandemic (Alsmadi et al., 2022). Therefore, increasing the level of responsible behaviour should occur for different population categories. Witsenboer et al. (2022) investigated the issue of personal cybersecurity in the school system, and based on the results, they suggested that cybersecurity education should start in elementary school, as the lack of relevant knowledge can affect them and the organization to which they belong. Also, students' awareness of cyber threats and risks has a positive effect in situations where students become targets of cybercrimes (Mohammed & Bamasoud, 2022). Older people tend to share their passwords, which creates a favourable environment for cyber criminals (Patel & Doshi, 2022). Therefore, this category of IT users needs unique approaches for forming special knowledge on personal cyber protection.

As for businesses and government institutions, the formation of responsible user behaviour should become vital in ensuring cyber protection. Boritz et al. (2022) proved that employees who are accountable for cybersecurity are less likely to become victims of cyber crimes. At the same time, bank employees are more susceptible to phishing than employees of professional services companies. Also, highly motivated public institution employees with a high level of responsiveness and self-efficacy contribute to ensuring reliable information protection (Sulaiman et al., 2022).

To increase the level of responsibility, it is vital to promote users' motivational behaviour to protect themselves and companies from cyber threats (Li et al., 2022). One should also be aware that a person's activities on the Internet can have a digital footprint that can lead to distortion of information about him and help cybercriminals (Nicol et al., 2022). Therefore, cyber hygiene should be observed, i.e. changing passwords, updating software, limiting the disclosure of personal information on social networks, etc. (Schoenherr & Thomson, 2021). Since not only individuals but also companies must be responsible for the security of their customers' data, protection methods must evolve towards using more reliable and advanced technologies. For example, the individual characteristics of a person typing on a keyboard, moving a cursor using a mouse, trackball, touchpad, etc., are unique and difficult to steal (Nnamoko et al., 2022). Therefore, implementing biometric technologies in online and mobile applications will reduce users' vulnerability to cyber criminals. For easy perception of

cybersecurity information, it is possible to use computer games to teach different categories of the population about personal protection (Hwang & Helser, 2022). Although the level of cybersecurity is formed under the influence of many factors, the responsible behaviour of IT users may be the critical aspect that will create favourable or unfavourable conditions for developing cybercrime.

CONCLUSIONS

The consequences of Industry 4.0 have had a positive impact on the life of society, which is manifested in the economic growth of the countries, increasing business efficiency, and improving the quality of individuals' lives. The results of the literature review confirm these facts. But scientific and technical progress also causes cybercrime, showing in the illegal appropriation of personal and financial information, violation of the software and technical support functioning. Therefore, the issue of ensuring cybersecurity is relevant for IT users, companies, and the government. In this research, it is stated that in the processes of digitization and informatization, a person is a crucial link, and his behaviour in the computer environment affects the level of cyber protection. The more responsible an individual is about cyber safety, especially personal security, the less likely he is to become a cyber victim.

The article, based on a survey of IT users from the European Union, confirmed the existence of a high correlation between cybercrime cases and indicators characterizing the responsible behaviour of individuals. At the same time, the impact of cybercrime cases is more significant on the choice of security measures. The number of users applying personal security measures will increase with growing cybercrime cases. All variables characterizing cases of cybercrimes proved essential for the respondents, indicating the expansion of cyber threats and the increase in the types of cyber victims. The authors found that the most significant contribution to the responsible behaviour of IT users will be made by such security measures as using at least four identification procedures and a procedure involving the mobile phone, restricting or refusing access to the geographical location, limiting access to profile or content on social networking sites or shared online storage, checking the security of the website where personal data is provided, understanding that cookies can be used to trace movements of people on the Internet. The results showed a slight influence of such variables as using other electronic identification procedures, single-use PIN code lists or random characters of a password, the software that limits the ability to track the activities on the internet, electronic identification certificate or card with a card reader or an app, simple login with username and password and refusing to allow the use of personal data for advertising purposes. The obtained results will enable us to conclude that the growth of cybercrimes determines the choice of security measures, and their application will not guarantee the complete freedom of IT users from various types of cyber threats.

The second part of the study concerned the construction of Kohonnen maps to identify regions characterized by the responsible or irresponsible behaviour of individuals to ensure personal cyber protection. As a result, 9 clusters were identified and substantiated using Silhouette Scores. Romania, Bulgaria, Serbia, Albania, North Macedonia and Bosnia and Herzegovina are countries whose respondents' behaviour can be characterized as the least responsible. IT users of Montenegro, Lithuania, Greece, Slovenia, Slovakia, Italy, Poland, and

Kosovo behave more responsibly concerning personal cyber protection than the respondents of the previous cluster. Still, they can also be classified as those who need to be more attentive to cybersecurity. It was found that a high level of responsible behaviour is characteristic of IT users from Denmark, Iceland, the Netherlands, the United Kingdom, Norway, Finland and Austria. The reliability of the cluster analysis is confirmed by the study of average values and the distribution of each type of individual cyber activity in the clusters.

The obtained results may be of interest primarily to international organizations engaged in developing a sustainable development strategy to ensure a safe and reliable cyberspace for the entire world, as well as for countries, businesses, and individuals. Also, they can become the basis for improving the population's digital and cyber literacy programs, which are developed and implemented by educational institutions and relevant centres engaged in professional development and training.

The main limitation of this study is obtaining survey data from respondents. The article is localized with the results provided by the European Commission, so it is impossible to conclude the behaviour of IT users from other countries. Also, the range of cybercrime cases and personal cyber protection tools that shape the appropriate behaviour of individuals is represented only by official data. It does not allow the conclusion about the different categories of respondents and consider various aspects of the IT users' responsible behaviour, which include psychological, social, economic, and other factors.

It is advisable to focus future research on studying the following questions. Firstly, a potential direction is the assessment of risks associated with non-compliance or inappropriate application of personal protection measures and identification of expected consequences for IT users. Emphasis should be placed on different groups of individuals - ordinary users, company employees, decision-makers, officials, etc. The obtained results will contribute to the formation of more precise preventive measures that will reduce the risk of cyber threats in a specific situation. Secondly, the next direction is the study of psychological and social factors that can affect the vulnerability of IT users, for example, emotional state, level of education, communication activity in social networks, level of digital and cyber literacy, trust in outsiders and their actions, etc. The potential results will identify the most critical factors for IT users that cybercriminals can use in the process of cybercrime. This knowledge should be taken into account, for example, by representatives of e-commerce or banks in the process of improving security measures in online or mobile applications.

FUNDING

This research was performed within the framework of state budget research: No 0121U109559 “National security through the convergence of financial monitoring systems and cybersecurity: intelligent modeling of financial market regulation mechanisms”, No 0123U101945 “National security of Ukraine through the prevention of financial fraud and money laundering: war and post-war challenges”, No 0121U109553 “Convergence of economic and educational transformations in the digital society: modelling of the impact on regional and national security”.

REFERENCES

Ahmed, R. R., Streimikiene, D., Channar, Z. A., Soomro, R. H., & Streimikis, J. (2021). E-Banking Customer Satisfaction and Loyalty: Evidence from Serial Mediation through Modified ES-QUAL Model and Second-Order PLS-SEM. *Engineering Economics, 32*(5), 407–421. https://doi.org/10.5755/j01.ee.32.5.28997

Alimbaev, A., Bitenova, B. A. G. D. A. T., & Bayandin, M. A. R. A. T. (2021). Information and Communication Technologies in the Healthcare System of the Republic of Kazakhstan: Economic Efficiency and Development Prospects. *Montenegrin J. Econ, 17*, 145–156. https://doi.org/10.14254/1800-5845/2021.17-3.12

Alsmadi, D., Maqousi, A., & Abuhussein, T. (2022). Engaging in cybersecurity proactive behavior: awareness in COVID-19 age. *Kybernetes*, (ahead-of-print). http://doi.org/10.1108/K-08-2022-1104

Beňo, M. (2022). Estimating E-workability Components Across Central European Countries. *AGRIS on-line Papers in Economics and Informatics, 14*(3), 3–16. https://doi.org/10.7160/aol.2022.140301

Bischoff, P. (2022, February 3). Cybercrime victims lose an estimated $318 billion annually. *Comparitech* [online]. Retrieved on December 1, 2022, from https://www.comparitech.com/blog/vpn-privacy/cybercrime-cost/

Boritz, J. E., Ge, C., & Patterson, K. (2022). Factors Affecting Employees' Susceptibility to Cyber-Attacks. *Journal of Information Systems, 36*(3), 27–60. http://doi.org/10.2308/ISYS-19-053

Capolupo, N., Palumbo, R., & Adinolfi, P. (2022). All that glitters is not gold. Exploring virtual team adoption in the COVID-19 era. *International Journal of Entrepreneurial Knowledge, 10*(1), 46–64. https://doi.org/10.37335/ijek.v10i1.148

Chen, P.-K., He, Q.-R., & Chu, S. (2022). Influence of blockchain and smart contracts on partners' trust, visibility, competitiveness, and environmental performance in manufacturing supply chains. *Journal of Business Economics and Management, 23*(4), 754–772. https://doi.org/10.3846/jbem.2022.16431

Constantinescu, R., & Edu, T. (2022). Internet of Things (IoT) as an Instrument to Improve Business and Marketing Strategies. A Literature Review. *European Journal of Interdisciplinary Studies, 14*(2). 143–154. http://doi.org/10.24818/ejis.2022.2

Cukier, M. (2007, February 9). Study: Hackers Attack Every 39 Seconds. *University of Maryland* [online]. Retrieved on December 1, 2022, from https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds

Davidovitch, N., & Eckhaus, E. (2022). Economics of time: Advantages of elearning in proportion to the time utilized and the tradeoff between work and studies. *Economics and Sociology, 15*(2), 222–235. https://doi.org/10.14254/2071-789X.2022/15- 2/14

Dečman, M., Stare, J., & Klun, M. (2022). The impact of the COVID-19 crisis on the development of the information society in Slovenia. *Administratie si Management Public, 39*, 77–96. https://doi.org/10.24818/amp/2022.39-05

Eurostat (2022a). Identification procedures used for online services (2020 onwards). *Eurostat* [online]. Retrieved on on December 1, 2022, from https://ec.europa.eu/eurostat/databrowser/view/ISOC_CISCI_IP20/default/table?lang=en&category=isoc.isoc_i.isoc_ci_sci

Eurostat (2022b). Privacy and protection of personal data (2020 onwards). *Eurostat* [online]. Retrieved on December 1, 2022, from https://ec.europa.eu/eurostat/databrowser/view/ISOC_CISCI_PRV20__custom_6994303/default/table?lang=en

Eurostat (2022c). Security related problems experienced when using the Internet. *Eurostat* [online]. Retrieved on December 1, 2022, from

https://ec.europa.eu/eurostat/databrowser/view/ISOC_CISCI_PB/default/table?lang=en&category=isoc.isoc_i.isoc_ci_sci

Federal Bureau of Investigation (2020). 2020 Internet Crime Report. *Federal Bureau of Investigation* [online]. Retrieved on on December 31, 2022, from https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Fleck, A. (2022, December 2). Cybercrime Expected to Skyrocket in Coming Years. *Statista* [online]. Retrieved on December 31, 2022, from https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

Florek, M., & Lewicki, M. (2022). Destinations, virtual reality and COVID-19. How isolation has shaped the behaviours and attitudes towards VR. *Economics and Sociology, 15*(1), 205–221. https://doi.org/10.14254/2071-789X.2022/15-1/13

Fülöp, M. T., Topor, D. I., Ionescu, C. A., Căpușneanu, S., Breaz, T. O., & Stanescu, S. G. (2022). Fintech accounting and Industry 4.0: future-proofing or threats to the accounting profession?. *Journal of Business Economics and Management, 23*(5), 997–1015. https://doi.org/10.3846/jbem.2022.17695

Gad, S., & Yousif, N. B. A. (2021). Public management in the education sphere: Prospects for realizing human capital in the development of knowledge management technologies. *Administratie si Management Public, 37*, 151–172. https://doi.org/10.24818/amp/2021.37-10

Gavrilović, A. (2018, October 30). [Webinar summary] 'What is responsible behaviour in cyberspace?' *Diplo* [online]. Retrieved on December 31, 2022, from https://www.diplomacy.edu/blog/webinar-what-responsible-behaviour-cyberspace/#:~:text=Defining%20responsible%20behaviour%20in%20cyberspace&text=Within%20the%20project%20team%2C%20the,that%20actor%20in%20those%20circumstances

Gladden, M., Fortuna, P., & Modliński, A. (2022). The Empowerment of Artificial Intelligence in Post-Digital Organizations: Exploring Human Interactions with Supervisory AI. *Human Technology*, *18*(2), 98–121. https://doi.org/10.14254/1795-6889.2022.18-2.2

Haddad, H. (2021). The Effect of Artificial Intelligence on the AIS Excellence in Jordanian Banks. *Montenegrin Journal of Economics, 17*(4), 155–166. https://doi.org/10.14254/1800-5845/2021.17-4.14

Hassan, M. M., & Lee, G. (2021). Online payment options and consumer trust: determinants of e-commerce in Africa. *International Journal of Entrepreneurial Knowledge*, *9*(2), 1–13. https://doi.org/10.37335/ijek.v9i2.121

Hogeveen, B. (2022, March 22). The UN norms of responsible state behaviour in cyberspace. *Australian Strategic Policy Institute* [online]. Retrieved on December 31, 2022, from https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace

Hwang, M. I., & Helser, S. (2022). Cybersecurity educational games: a theoretical framework. *Information & Computer Security*, *30*(2), 225–242. http://doi.org/10.1108/ICS-10-2020-0173

Kiba-Janiak, M., Cheba, K., Mucowska, M., & de Oliveira, L. K. (2022). Segmentation of e-customers in terms of sustainable last-mile delivery. *Oeconomia Copernicana*, *13*(4), 1117–1142. https://doi.org/10.24136/oc.2022.032

Kohonen, T., & Honkela, T. (2007). Kohonen network. *Scholarpedia*, *2*(1), 1568. https://doi.org/10.4249/scholarpedia.1568

Kobis, P., & Karyy, O. (2021). Impact of the human factor on the security of information resources of enterprises during the COVID-19 pandemic. *Polish Journal of Management Studies*, *24*(2), 210–227. https://doi.org/10.17512/pjms.2021.24.2.13

Kolosok, S., Lyeonov, S., Voronenko, I., Goncharenko, O., Maksymova, J., & Chumak, O. (2022). Sustainable business models and IT innovation: The case of the REMIT. *Journal of Information Technology Management, 14*, 147–156. https://doi.org/10.22059/JITM.2022.88894

Kreyszig, E. (1979). *Advanced Engineering Mathematics (Fourth ed.).* New York City, United States: John Wiley and Sons Ltd.

Krsek, I., Wenzel, K., Das, S., Hong, J. I., & Dabbish, L. (2022). To self-persuade or be persuaded: Examining interventions for users' privacy setting selection. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (pp. 1-17). http://doi.org/10.1145/3491102.3502009

Kuzior, A., Vasylieva, T., Kuzmenko, O., Koibichuk, V., & Brożek, P. (2022). Global digital convergence: Impact of cybersecurity, business transparency, economic transformation, and AML efficiency. *Journal of Open Innovation: Technology, Market, and Complexity, 8*(4). https://doi.org/10.3390/joitmc8040195

León-Gómez, A., Santos-Jaén, J. M., Ruiz-Palomo, D., & Palacios-Manzano, M. (2022). Disentangling the impact of ICT adoption on SMEs performance: the mediating roles of corporate social responsibility and innovation. *Oeconomia Copernicana, 13*(3), 831–866. https://doi.org/10.24136/oc.2022.024

Li, L., Xu, L., & He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. *Computers in Human Behavior Reports, 5*, 100165. http://doi.org/10.1016/j.chbr.2021.100165

Lustigova, Z., Jarolímková, L., & Žufan, J. (2021). Evaluation of Tourist Decision-Making Process by Eye-Tracking Method – Focused on Methodology Gap and Cross-National Comparison. *Journal of Tourism and Services, 12*(22), 89–104. https://doi.org/10.29036/jots.v12i22.258

Lydeka, Z., & Karaliute, A. (2021). Assessment of the effect of technological innovations on unemployment in the European Union Countries. *Engineering Economics, 32*(2), 130–139. https://doi.org/10.5755/j01.ee.32.2.24400

MacKay, J. (2022). Why Cyber Security Is Everyone's Responsibility. *MetaCompliance* [online]. Retrieved on December 31, 2022, from https://www.metacompliance.com/blog/cyber-security-awareness/why-cyber-security-is-everyones-responsibility

Millia, H., Adam, P, Muhatlib, A. A., Tajuddin, & Pasrun, Y. P. (2022). The Effect of Inward Foreign Direct Investment and Information and Communication Technology on Economic Growth in Indonesia. *AGRIS on-line Papers in Economics and Informatics, 14*(1), 69-79. http://doi.org/10.7160/aol.2022.140106

Mnohoghitnei, I., Horobeț, A., & Belaşcu, L. (2022). Bitcoin is so Last Decade – How Decentralized Finance (DeFi) could Shape the Digital Economy. *Eur. J. Interdiscip. Stud, 14*, 87–99. http://doi.org/10.24818/ejis.2022.06

Mohammed, M. A. R. A. M., & Bamasoud, D. M. (2022). The Impact of Enhancing Awareness of Cybersecurity on Universities Students: A Survey Paper. *Journal of Theoretical and Applied Information Technology, 100*(15), 4756–4766

Navickas, V., Grencikova, A., Kordos, M., & Sramka, M. (2022). The information and communications technologies' usage within the COVID-19 pandemic issue. *Transformations in Business & Economics, 21*(1), 101–113

Nicol, E., Briggs, J., Moncur, W., Htait, A., Carey, D. P., Azzopardi, L., & Schafer, B. (2022). Revealing cumulative risks in online personal information: a data narrative study. *Proceedings of the ACM on Human-Computer Interaction, 6*(CSCW2), 1–25. http://doi.org/10.1145/3555214

Nnamoko, N., Barrowclough, J., Liptrott, M., & Korkontzelos, I. (2022). A behaviour biometrics dataset for user identification and authentication. *Data in Brief, 45*, 108728. https://doi.org/10.1016/j.dib.2022.108728

Okunevičiūtė Neverauskienė, L., Novikova, M., & Kazlauskienė, E. (2021). Factors determining the development of intelligent transport systems. *Business, Management and Economics Engineering*, *19*(2), 229–243. https://doi.org/10.3846/bmee.2021.15368

Oliveira, E., & Baldi, V. (2022). Systematic Review on Cybersecurity Risks and Behaviours: Methodological Approaches. In *Proceedings of the International Conference on Complexity, Future Information Systems and Risk, COMPLEXIS* (pp. 49–56). Portugal: SciTePress. http://doi.org/10.5220/0010762600003197

Orson, L., & Stein, S. (2020). *The new imperative for corporate data responsibility*. Delaware, the U.S.: KPMG LLP.

Patel, S., & Doshi, N. (2022). Internet of Behavior in Cybersecurity: Opportunities and Challenges. In *Futuristic Trends in Networks and Computing Technologies: Select Proceedings of Fourth International Conference on FTNCT 2021* (pp. 219-227). Singapore: Springer Nature Singapore.

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: an integrated methodological approach. *Cognition, Technology & Work*, *24*(2), 371–390. http://doi.org/10.1007/s10111-021-00683-y

Popov, V., Medineckienė, M., Grigorjeva, T., & Zabulėnas, A. R. (2021). Building information modelling: procurement procedure. *Business, Management and Economics Engineering*, *19*(1), 180–197. https://doi.org/10.3846/bmee.2021.14653

Rapp, N., & Hackett, R. (2017, October 25). A Hacker's Tool Kit. *Fortune* [online]. Retrieved on December 31, 2022, from https://fortune.com/2017/10/25/cybercrime-spyware-marketplace/

Remeikiene, R., Gaspareniene L., Fedajev, A., & Vebraite, V. (2021). The role of ICT development in boosting economic growth in transition economies. *Journal of International Studies, 14*(4), 9–22. https://doi.org/10.14254/2071-8330.2022/14-4/1

Rosenberg, D., & Taipale, S. (2022). Social and satisfied? Social uses of mobile phone and subjective wellbeing in later life. *Human Technology*, *18*(1), 45–65. https://doi.org/10.14254/1795-6889.2022.18-1.4

Rousseeuw, P. J. (1987). Silhouettes: a Graphical Aid to the Interpretation and Validation of Cluster Analysis. *Computational and Applied Mathematics, 20,* 53–65. https://doi.org/10.1016/0377-0427(87)90125-7

Schoenherr, J. R., & Thomson, R. (2021). The cybersecurity (CSEC) questionnaire: Individual differences in unintentional insider threat behaviours. In *2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1-8). IEEE. http://doi.org/10.1109/CyberSA52016.2021.9478213

Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks. *Information*, *13*(9), 413. http://doi.org/10.3390/info13090413

Surfshark (2022). Cybercrime statistics. *Surfshark* [online]. Retrieved on December 31, 2022, from https://surfshark.com/research/data-breach-impact/statistics

Tiutiunyk, I., Drabek, J., Antoniuk, N., Navickas, V., & Rubanov, P. (2021). The impact of digital transformation on macroeconomic stability: Evidence from EU countries. *Journal of International Studies, 14*(3), 220–234. https://doi.org/10.14254/2071- 8330.2021/14-3/14

Tran, L. Q. T., Phan, D. T., Herdon, M., & Kovacs, L. (2022). Assessing the Digital Transformation in Two Banks: Case Study in Hungary. *AGRIS on-line Papers in Economics and Informatics, 14*(2), 121–134. https://doi.org/10.7160/aol.2022.140210

Tugui, A., Jeflea, F. V., Opariuc, C., Filipeanu, D., & Agheorghiesei, D. T. (2022). Societal transformations in Romanian society: humanity's interaction with artificial intelligence towards the technological singularity. *Transformations in Business & Economics, 21*, 435–461.

Vasilyeva, T., Kuzmenko, O., Stoyanets, N., Artyukhov, A., & Bozhenko, V. (2022). The depiction of cybercrime victims using data mining techniques. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu, 5*, 174–178. https://doi.org/10.33271/nvngu/2022-5/174

Witsenboer, J. W. A., Sijtsma, K., & Scheele, F. (2022). Measuring cyber secure behavior of elementary and high school students in the Netherlands. *Computers & Education*, *186*, 104536. http://doi.org/10.1016/j.compedu.2022.104536

World Economic Forum (2022). *The Global Risks Report 2022 17th Edition*. Cologny/Geneva, Switzerland: World Economic Forum.

Zamir, Z., & Kim, D. (2022). The effect of quality dimensions of information systems on knowledge sharing and user satisfaction. *International Journal of Entrepreneurial Knowledge*, *10*(1), 1–19. https://doi.org/10.37335/ijek.v10i1.153

Authors' Note

All correspondence should be addressed to
Zoltán Szira
Budapest Metropolitan University,
Budapest, Hungary
ORCID 0000-0002-7299-4695
zszira@metropolitan.hu

Human Technology
ISSN 1795-6889
https://ht.csr-pub.eu

Appendix A

Results of factor structures and canonical weights

Variable	Factor Structure, right set							
	Root 1	Root 2	Root 3	Root 4	Root 5	Root 6	Root 7	Root 8
Using a simple login with username and password	0.7275	0.0062	0.2535	0.1502	0.1615	-0.1639	0.1353	-0.0983
Using a social media login	0.7418	0.0123	-0.0435	0.0706	-0.0852	-0.1544	-0.3002	-0.0818
Using a security token	0.6852	-0.1391	0.4003	0.0295	-0.1462	0.1254	0.0780	-0.3447
Using an electronic identification certificate or card with a card reader or an app	0.6107	0.0216	-0.1726	0.2098	0.0914	0.1279	0.1832	0.2248
Using a procedure involving the mobile phone	0.8404	-0.1283	0.1629	0.1178	0.0791	-0.0733	-0.0379	-0.0975
Using a single-use PIN code list or random characters of a password	0.5952	0.2725	-0.2600	0.2596	-0.1724	-0.1978	-0.0605	-0.2053
Using other electronic identification procedures	0.5866	-0.0468	-0.1715	-0.0653	-0.1044	-0.4235	-0.1569	-0.3725
Using at least 4 identification procedures	0.9480	0.0064	0.0099	0.0974	-0.1696	-0.0917	0.0058	-0.0201
Individuals know that cookies can be used to trace the movements of people on the Internet	0.6780	0.0450	-0.0971	0.1870	-0.0811	0.1644	0.2527	-0.3110
Changing the settings in the internet browser to prevent or limit cookies on any devices	0.5163	0.1489	0.1407	0.3938	0.0139	-0.1462	0.2759	-0.1350
Using software that limits the ability to track the activities on the Internet	0.6442	-0.0549	0.0247	0.1999	-0.0910	-0.1836	0.0086	-0.1967
Reading privacy policy statements before providing personal data	0.1724	0.4170	0.3114	-0.1211	-0.0349	0.0095	0.2183	-0.4352
Restricting or refusing access to the geographical location	0.7421	0.2999	0.0883	0.0016	0.0046	0.1472	-0.0451	-0.0088
Limiting access to profiles or content on social networking sites or shared online storage	0.5173	0.0812	0.1681	0.1675	-0.1764	0.1213	-0.2000	-0.3251
Rejection of using personal data for advertising purposes	0.5362	0.1853	0.0816	0.2721	-0.1379	0.0887	-0.0739	-0.2948
Checking the security of the website where personal data is provided	0.6239	-0.1538	0.1830	0.3393	-0.1617	-0.0302	-0.0634	-0.1773

Figure 1. Factor structure of the right set characterizing the IT users' responsible behavior.
[Source: calculated by the authors]

Variable	Factor Structure, left set							
	Root 1	Root 2	Root 3	Root 4	Root 5	Root 6	Root 7	Root 8
Fraudulent credit or debit card use	0.8398	-0.0549	-0.1020	-0.1618	-0.3889	-0.2090	0.0037	-0.2453
Online identity theft	0.6504	-0.0228	0.4616	0.1571	-0.5029	-0.2055	-0.1332	-0.1606
Phishing	0.7750	0.3117	0.1648	0.2857	0.0522	0.1517	-0.1138	-0.3934
Pharming	0.7702	0.0133	0.2890	-0.1289	-0.4248	0.2528	-0.0852	-0.2341
Misuse of personal information available on the Internet	0.7648	-0.0175	0.2964	-0.0970	-0.0893	-0.3698	0.3882	0.1486
Social network or e-mail account being hacked	0.5812	-0.5956	0.3507	0.2777	0.0449	-0.0289	-0.1437	-0.2897
Data loss due to a virus	0.1008	-0.2835	0.0179	-0.1569	-0.2469	-0.3174	0.8248	-0.2062
Identity theft, receiving fraudulent messages or being redirected to fake websites	0.8285	0.0016	-0.2763	0.3125	-0.2698	0.2546	0.0258	0.0368

Figure 2. Factor structure of the left set characterizing cases of cybercrime.
[Source: calculated by the authors]

Variable	Canonical Weights, right set							
	Root 1	Root 2	Root 3	Root 4	Root 5	Root 6	Root 7	Root 8
Using a simple login with username and password	0.0651	0.0869	0.0363	0.3738	1.0141	-0.7187	-0.0951	0.0064
Using a social media login	0.1782	0.3464	0.0815	0.3232	0.5801	0.2880	-0.5661	0.0417
Using a security token	0.1688	0.1573	0.4065	0.6672	1.1148	0.8591	-0.3190	-0.9391
Using an electronic identification certificate or card with a card reader or an app	-0.0410	0.5157	-0.5853	1.2713	1.4733	0.5971	-0.2054	-0.5930
Using a procedure involving the mobile phone	0.3602	-0.7199	0.3399	-0.4942	0.8296	0.3046	-0.4228	-0.2041
Using a single-use PIN code list or random characters of a password	0.0087	0.4143	-0.8250	1.1622	0.9228	0.2255	-0.2568	-0.7530
Using other electronic identification procedures	-0.0043	-0.1619	-0.5994	-0.4002	0.9391	-0.6570	-0.2051	-0.7557
Using at least 4 identification procedures	0.3972	0.1799	0.9708	-1.7964	-4.9879	-1.3866	0.8463	2.3949
Individuals know that cookies can be used to trace the movements of people on the Internet	0.2342	-1.1448	-1.1725	-0.9201	-0.1718	0.8631	1.2506	-0.4715
Changing the settings in the internet browser to prevent or limit cookies on any devices	-0.0985	0.4340	1.0568	0.2539	0.0320	-0.6453	0.0728	0.3060
Using software that limits the ability to track the activities on the Internet	-0.0191	-0.1229	-0.1019	-0.0986	-0.3712	-0.3548	0.1609	-0.4599
Reading privacy policy statements before providing personal data	-0.1552	0.5593	0.2738	-0.2357	-0.4510	-0.1980	0.8739	-0.3032
Restricting or refusing access to the geographical location	0.3515	0.2555	-0.3204	-0.7235	1.5855	0.7127	0.0093	0.3431
Limiting access to profiles or content on social networking sites or shared online storage	-0.2733	-0.2203	0.6234	-0.4786	-0.4317	0.0656	-1.6637	-0.9600
Rejection of using personal data for advertising purposes	0.0404	1.5063	0.2425	1.0828	-1.0620	-0.0239	-0.7246	0.5950
Checking the security of the website where personal data is provided	-0.2598	-1.3011	-0.5101	1.1490	0.2125	0.2024	1.2212	0.3140

Figure 3. Canonical weights for the right set characterizing the IT users' responsible behavior
[Source: calculated by the authors]

Variable	Canonical Weights, left set							
	Root 1	Root 2	Root 3	Root 4	Root 5	Root 6	Root 7	Root 8
Fraudulent credit or debit card use	0.3745	-0.1452	-1.2003	-0.9257	0.0359	-1.1507	-0.8632	-0.7419
Online identity theft	-0.4745	0.3961	0.5340	1.2503	-1.3537	-0.8327	-0.2824	0.0917
Phishing	0.1466	0.9631	0.0993	0.4957	0.7107	-0.0994	0.3000	-1.1193
Pharming	0.1599	-0.1874	0.7936	-1.3122	-0.2376	1.6642	0.2402	0.0869
Misuse of personal information available on the Internet	0.6336	0.1453	0.5347	-0.4704	0.8055	-0.2516	0.3073	1.1667
Social network or e-mail account being hacked	0.1949	-1.1461	0.1512	0.1183	0.5834	0.0643	-0.2493	-0.2005
Data loss due to a virus	-0.3131	-0.0834	-0.0183	0.3491	-0.4064	0.1417	1.0377	-0.7364
Identity theft, receiving fraudulent messages or being redirected to fake websites	0.2306	-0.2105	-0.6307	1.0219	-0.5209	0.5359	0.3577	0.7995

Figure 4. Canonical weights for the left set characterizing cybercrime cases
[Source: calculated by the authors]

Appendix B

The calculated average values of indicators

Table 1. Average values of the indicators in accordance with the cluster profile.

Indicator	C1*	C2	C3	C4	C5	C6	C7	C8	C9
Using a simple login with username and password	65.3700	76.4200	46.2200	70.7000	71.1400	84.3600	71.3100	89.4200	74.0400
Using a social media login	32.7300	37.2100	20.1600	42.6600	28.7000	46.6400	36.8300	49.4700	30.2000
Using a security token	15.3000	13.0600	4.2800	24.1400	15.6500	29.5600	23.2400	58.0000	6.6200
Using an electronic identification certificate or card with a card reader or an app	14.5800	27.9400	2.3300	32.9400	10.7200	65.8900	44.8200	22.8500	12.4000
Using a procedure involving the mobile phone	31.5000	55.7200	12.0800	52.6000	34.5300	76.8400	42.2100	73.7800	57.1700
Using a single-use PIN code list or random characters of a password	13.0100	13.5400	2.7100	20.2800	10.2200	44.6000	12.1500	32.9600	38.5400
Using other electronic identification procedures	5.4500	8.1800	1.8300	11.5900	3.0900	16.4500	5.4000	13.7100	7.1600
Using at least 4 identification procedures	15.0400	22.9200	2.9400	33.2000	13.1600	58.0500	25.4900	48.2100	18.6500
Individuals know that cookies can be used to trace movements of people on the Internet	50.9700	62.4000	34.4000	64.1000	74.3000	84.4600	70.1800	78.5000	80.3500
Changing the settings in the internet browser to prevent or limit cookies on any devices	22.2700	27.4500	14.8400	28.0000	27.7100	37.3800	35.6000	30.4200	43.8900
Using software that limits the ability to track the activities on the Internet	15.9000	14.3100	8.2500	22.1400	11.4500	27.3600	34.0500	25.9000	17.5100
Reading privacy policy statements before providing personal data	37.4500	37.6800	29.0400	40.0400	46.7700	40.0500	22.0800	40.0300	50.1700
Restricting or refusing access to the geographical location	31.0000	37.7000	24.4100	52.1800	49.2400	71.1500	35.9000	56.8500	63.6300
Limiting access to profiles or content on social networking sites or shared online storage	25.3700	36.6500	13.1500	47.7300	44.6100	51.2400	28.6900	41.0300	55.1600
Rejection of usingpersonal data for advertising purposes	31.4100	41.6600	16.4000	50.2400	57.5500	59.8000	39.4800	51.0400	65.2000
Checking the security of the website where personal data is provided	20.0400	40.0000	6.6700	43.5200	31.2000	49.9300	23.3200	43.3200	42.5500

*C means a cluster

[Source: calculated by the authors]

Appendix C

Kohonen maps

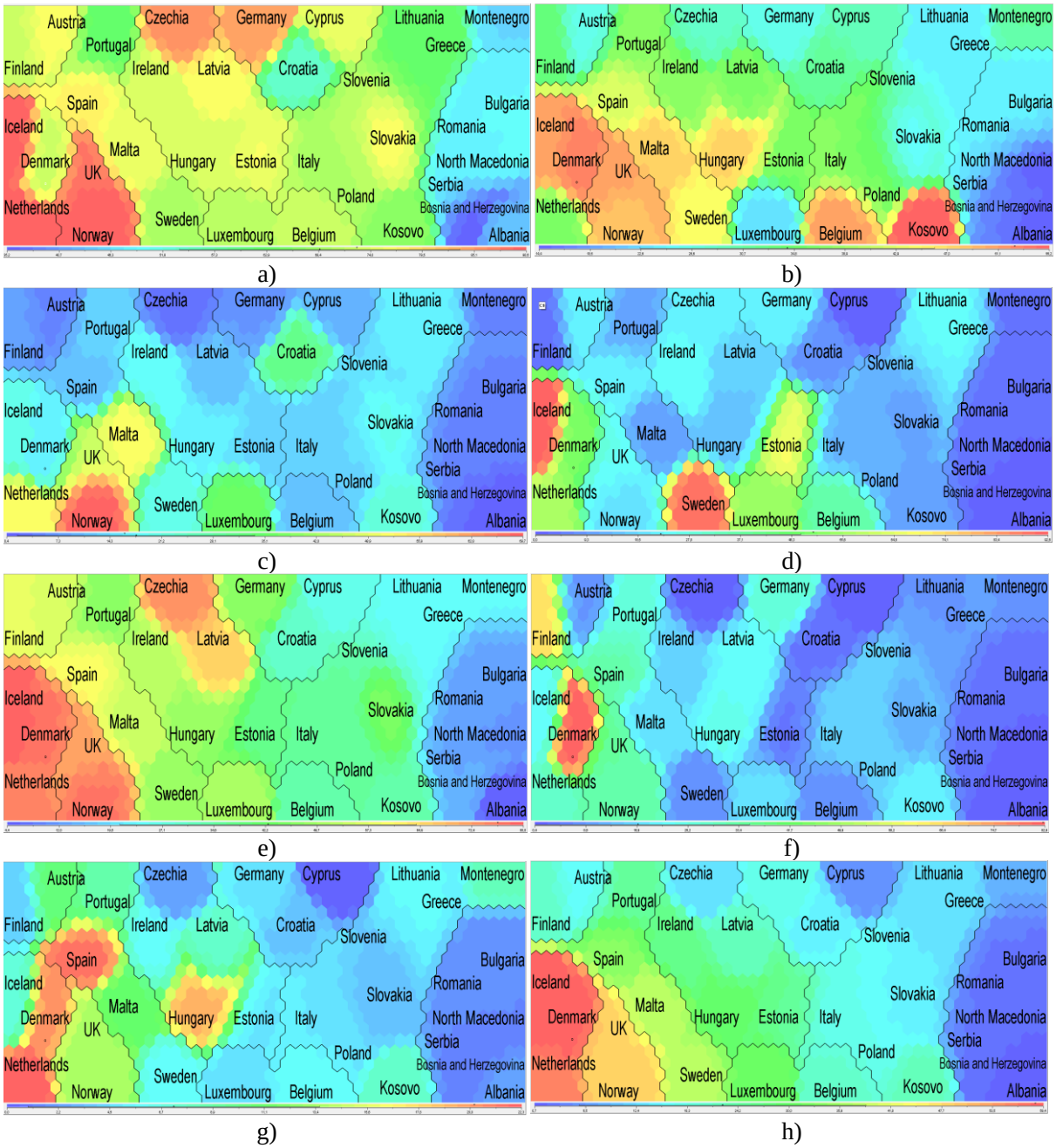


Figure 5. Kohonen maps for indicators characterizing the responsible behaviour of IT consumers: a) Using a simple login with username and password; b) Using a social media login; c) Using a security token; d) Using an electronic identification certificate or card with a card reader or an app; e) Using a procedure involving the mobile phone; f) Using a single-use PIN code list or random characters of a password; g) Using other electronic identification procedures; h) Using at least 4 identification procedures.
[Source: calculated by the authors]

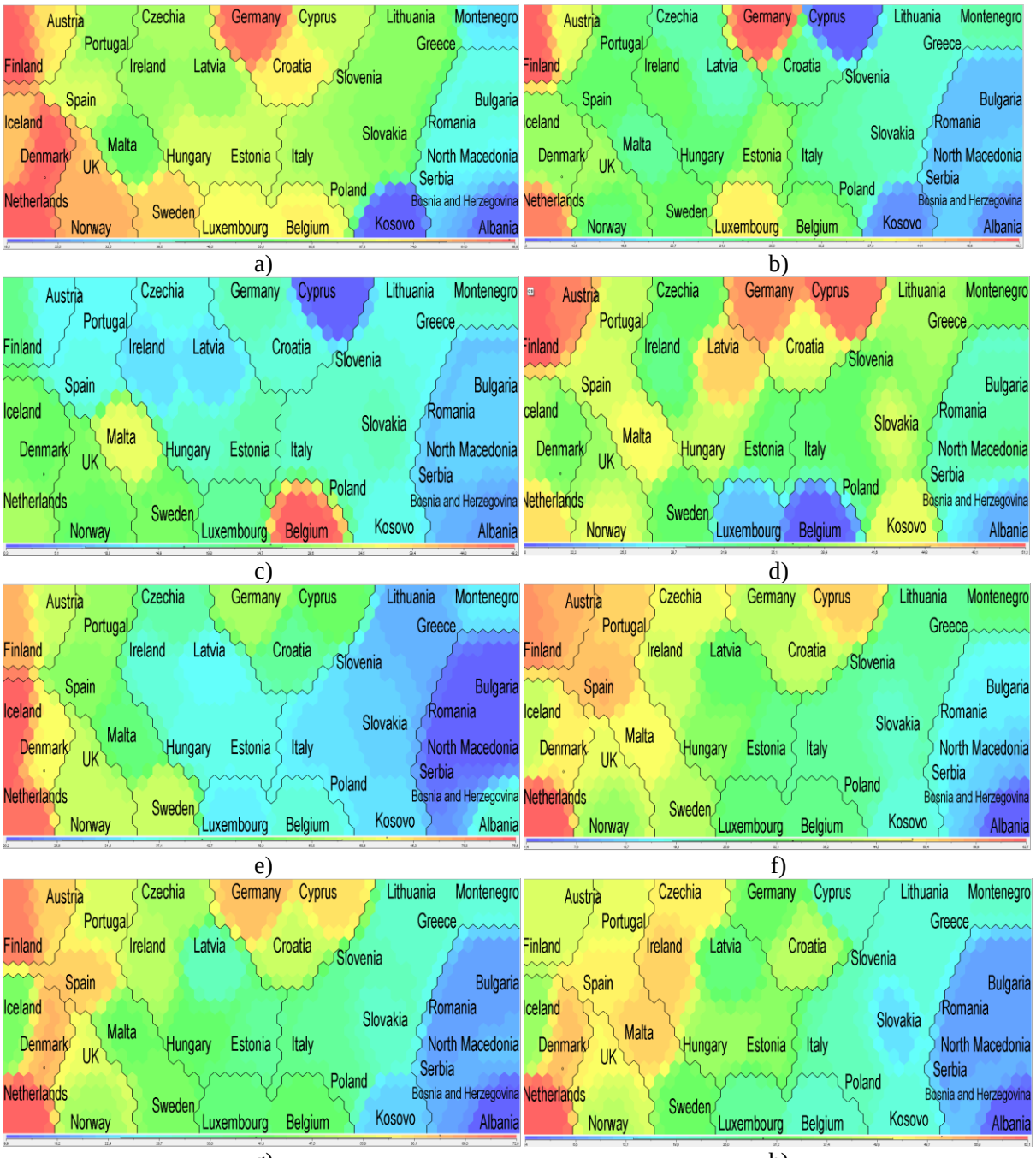


Figure 6. Kohonen maps for indicators characterizing the responsible behaviour of IT consumers: a) Individuals know that cookies can be used to trace the movements of people on the Internet; b) Changing the settings in the internet browser to prevent or limit cookies on any devices; c) Using software that limits the ability to track the activities on the Internet; d) Reading privacy policy statements before providing personal data; e) Restricting or refusing access to the geographical location; f) Limiting access to profiles or content on social networking sites or shared online storage; g) Rejection of using personal data for advertising purposes; h) Checking the security of the website where personal data is provided.
[Source: calculated by the authors]