sciendo

Economics and Business Review, Vol. 7 (21), No. 4, 2021: 94-120
DOI: 10.18559/ebr.2021.4.6

"Every knock is a boost". Cyber risk behaviour among Poles[1]

***Ewa Cichowicz*[2], *Małgorzata Iwanicz-Drozdowska*[3], *Łukasz Kurowski*[4]**

Abstract: The purpose of this study is to evaluate the safety of individuals' behaviour in the cyber world, especially when using financial services. The article focuses on knowledge of cybersecurity issues, cyber risk awareness and respondents' self-assessment as potential determinants of individual behaviour. The data obtained from a survey of a representative group of Polish citizens during the second wave of the COVID-19 pandemic was analysed. Ordinal logistic regression and instrumental variable analysis confirm the existence of a positive relationship between knowledge and awareness of cyber risk and safe behaviour in the cyber world. Older generations exhibit safer behaviour which may be linked to their life experience; however, the results do not confirm that experiencing a loss due to cyber risk convinces individuals to use Internet-based solutions in a safer manner. Therefore, educational campaigns should be expanded to include cyber risk issues and tailored to the needs of various users.

Keywords: cybersecurity behaviour, knowledge of cybersecurity, instrumental variables, financial services.

JEL codes: G51, D10, M15, P36.

[1] Article received 26 June 2021, accepted 1 December 2021. This work was supported by the SGH Warsaw School of Economics [KZIF/S20/1.11].

[2] Financial System Department, Collegium of Management and Finance, SGH Warsaw School of Economics, al. Niepodległości 162, 02-554 Warszawa, Poland, corresponding author: ewa.cichowicz@sgh.waw.pl, ORCID: https://orcid.org/0000-0002-9379-9127.

[3] Financial System Department, Collegium of Management and Finance, SGH Warsaw School of Economics, al. Niepodległości 162, 02-554 Warszawa, Poland, miwani@sgh.waw.pl, ORCID: https://orcid.org/0000-0002-8490-5178.

[4] Financial System Department, Collegium of Management and Finance, SGH Warsaw School of Economics, al. Niepodległości 162, 02-554 Warszawa, Poland, lukasz.kurowski@sgh.waw.pl, ORCID: https://orcid.org/0000-0002-3306-4276.

Introduction

Societies are becoming increasingly dependent on Internet-based solutions that provide various key services (including financial services and critical infrastructure, see Lis and Mendel (2019) for details). The scale and scope of the digital economy have grown in recent years. As indicated by Milošević, Dobrota and Barjaktarović Rakočević (2018) the digital economy contributes significantly to economic growth, especially in the European Union. The COVID-19 pandemic has further heightened the importance of the Internet and certain remote modes of work, study or life will persist for a long time after the pandemic. The lockdown period contributed to the creation of new mobile applications and digital channels that have enabled adaptation to new conditions. The boom in online shopping and contactless payment methods as well as the growing role of electronic banking services, has been a strong stimulus for the development of e-commerce. Business decisions, work and education schedules and even personal relationships not only involve but also increasingly rely on tools based on modern technologies. Therefore the behaviour of users in the cyber world are of high importance for social and economic safety.

As technology increasingly permeates everyday life consumers are becoming more vulnerable to cyber risks. According to a report by Javelin Strategy & Research and SAS (Tedder, 2020) the transfer of many processes to the digital space and changes in the way consumers interact with financial services and commerce have proved necessary (especially during the COVID-19 pandemic) but have contributed to an obvious increase in cyber attacks worldwide. Naidoo (2020) developed a multi-level influence model showing how cyber criminals are exploiting the COVID-19 pandemic. Although the impact of the wave of fraud related to the COVID-19 crisis is apparent in various areas of the economy undoubtedly one of the strongest determinants is the increase in the importance of digital channels related to electronic banking. Poorly protected financial accounts and unsafe online behaviour can facilitate the activity of cyber criminals. In the December 2020 edition of "Fraud in the Wake of COVID-19: Benchmarking Report" the Association of Certified Fraud Examiners (2020) released a survey result in which 79% of participants said they had seen an increase in the overall level of fraud (compared to 77% in August and 68% in May), and 88% expected a further increase in cyber fraud (as the top fraud risk in the opinion of the respondents) over the next year. Similar conclusions have been presented by the Bank for International Settlements (Aldasoro, Frost, Gambacorta, & Whyte, 2021).

Despite many attempts to define cyber risk in the literature no universal and coherent definition exists (Kosub, 2015). There are several reasons for this gap. One is the interdisciplinary nature of this type of risk. Another is the constant change in the forms of cyber risk which is related to ongoing technological progress as well as changes in laws and regulations as underlined by

Da Veiga (2018). Cybersecurity refers to technologies, processes and practices designed to protect information networks, devices, programs and data from hacking attacks, damage, or unauthorized access (Von Solms & Van Niekerk, 2013). Cybersecurity can be defined as information technology security and is applicable to banking services (e.g., e-banking). Cyber risk is a component of operational risk recognized in regulated financial and industrial (especially in key infrastructure) sectors. On the one hand the financial sector is expected to be well prepared for cyber attacks because of comprehensive regulations that mitigate operational risk. On the other, the behaviour of users plays an important role in the actual level of cyber risk. This situation emphasizes the need to conduct surveys to evaluate individuals' behaviour in the cyber world.

In Poland, which is the largest EU member from post-communist block, both society and the economy are characterized by increasing use of the Internet and well-developed electronic banking solutions and e-commerce. After the political and economic transformations began in the 1990s, Poland as with the whole CEE region, made substantial progress in the use of new technologies in business and society. In this case, starting from a lower level of development appeared to be an advantage. According to McKinsey (2020), CEE countries accelerated their digitalization process although European "digital frontrunners" transformed their economies even faster. Poland as a large market in the CEE is an interesting research object as a transition country undergoing a catch-up process. It should be noted that it is also a representative of maturing emerging markets.

The aim of this study is to evaluate how knowledge of cybersecurity issues, cyber risk awareness and self-assessment in this area affect the behaviour of Poles in the cyber world. The research claims that two pillars are important for reducing the impact of cyber risk. The first pillar is a combination of knowledge and awareness which is shaped by professional and private life. The second is related to bad experiences in the cyber world which may curb exposure to cyber risk as "every knock is a boost". To achieve the goal research propositions were operationalized into survey questions. Moreover, the survey pays attention to cyber risk losses faced by respondents and their role in improving the safety of behaviour in the cyber world to gain insights into the role of lessons learned in cybersecurity culture. This approach should allow the determination as to whether improvements in cybersecurity culture can be based solely on gained experience. It should be claimed that knowledge and awareness are necessary to build a reasonable cybersecurity culture. This approach is similar to the concept of Georgiadou, Mouzakitis, Bounas and Askounis (2020). According to their model, in the security culture two levels can be distinguished: organizational and individual. There are four dimensions at the individual level: attitude, awareness, behaviour and competency. This article focuses on the core human-related factors of security. Unlike Georgiadou and others (2020) the current research takes the perspective of an individual ex-

posed to cyber risk both in private and professional life and therefore draws attention to the need to counteract this risk to preserve the individual's well-being. The research makes several important contributions. First, it evaluates knowledge and awareness of cybersecurity in Polish society. This study is the first to use a large research sample ($n = 1804$) to verify the knowledge of Polish society in this area. Second, the results can be used to identify ways to reduce cyber risk (i.e., knowledge and awareness versus experience). Third the study is important for all Internet users since it highlights the role of education in preventing possible losses related to cyber risk.

The rest of the paper is arranged as follows. Section 1 provides a theoretical background that shows how cyber risk is dealt with in the relevant literature. Three main streams have been identified which are also related to human behaviour in the light of the existence of this risk. Section 2 presents how the research based on the CAWI survey was conducted and how the research propositions were operationalized and the methodology is explained. Section 3 provides detailed information on empirical findings in particular on knowledge, awareness and self-assessment and their relationship to cybersecurity behaviour in general and Internet banking specifically. The study finishes with conclusions.

1. Literature review

Many studies have noted the increasing presence of consumers on the web for purposes related not only to their professional work or education but also to everyday life. The literature review focuses on three streams of research. The first stream relates to measures undertaken by businesses to ensure cybersecurity, while the second evaluates the efficiency of educational campaigns related to cyber risk. The third focuses on customer behaviour on the Internet.

According to the first stream, companies attach great importance to introducing security measures to reduce cyber risk. This is especially true of financial institutions such as banks. However, the implementation of products designed to improve the level of security on a network does not automatically lead to cybersecurity. Security measures are often ineffective because consumers do not behave in the manner necessary to ensure cybersecurity (e.g., by sharing their passwords or not using anti-virus programs). Accordingly, there is a widespread view that the weakest link in cybersecurity is humans (Hughes-Larteya, Li, Botchey, & Qin, 2021). During the pandemic and successive lockdowns the situation worsened further as criminals intensified cyber attacks, by exploiting the chaos of abnormal conditions and the increase in working from home using home computers.

The literature increasingly points to a more comprehensive approach to cybersecurity in organizations (Hussain, Mohamed, & Razali, 2020). This kind of approach recognizes that cybersecurity also needs to be addressed through or-

ganizational and not just technical measures. Reegård, Blackett and Katta (2019) conclude that the cybersecurity culture is a subcomponent of organizational culture consisting of layers that are becoming increasingly visible. A survey of employees by Parsons and others (2015) reveals a significant, positive relationship between information security decision making and an organizational information security culture. This means that improving an organization's security culture translates into employees' behaviour in the field of cybersecurity.

The study on motivating employees to take actions to mitigate cyber risk by S. R. Boss, Kirsch, Angermeier, Shingler and R. W. Boss (2019) indicates the impact of reward and sanction policies. Yasin, Liu, Li, Wang and Zowghi (2018) recognize that it is essential for cybersecurity to be understood by all stakeholders in an organization. They draw attention to the fact that the involvement of stakeholders in maintaining safety rules is invariably insufficient. The use of innovative tools based on games, films or media productions could contribute to a change in this area by making the whole process more fun and enjoyable which would increase the involvement of employees and their internal motivation. Therefore, game-based learning not only leads to knowledge gains but also enables the acceleration of the entire process thus increasing the commitment and satisfaction of learners. Similar observations have been made in the case of quality management and overall operational risk management. The construction of a cybersecurity culture may be supported by experiences from other issues that were introduced one or even two decades ago.

In the second stream of research, relevant studies analyse possibilities for training and education related to improving cybersecurity. I. M. Venter, Blignaut, Renaud and M. A. Venter (2019) distinguish two general steps in cybersecurity education: first people must become aware of the need to take cyber risk mitigation measures; second teachers need to impart the skills required to take the necessary precautions. Junger, Montoya and Overink (2017) analyse various tools to improve the awareness of web users. They note that there is no clear evidence of the effectiveness of warnings although there are principles that can improve their effectiveness. Such guidelines have been considered by, e.g., Wogalter, Laughery Sr. and Mayhorn (2012), who emphasize, *inter alia*, that warnings should not be addressed to the "average person" but should be structured in such a way as to reach people with poorer education, lower knowledge, weaker competences, etc.

Encouraging users to behave safely on the Internet is difficult. For example, Yildirim and Mackie (2019) argue that while most people are aware of the importance of choosing strong passwords the password policy used is often not sufficient to motivate users to choose such passwords. The results of a study by Grazioli and Wang (2001) indicate that many unsophisticated users are exposed to cyber risk and are unable to effectively integrate the information they gather. Consequently progress may be achieved when it is possible to educate individuals to better evaluate clues to deception. According to an overview by

Junger and others (2017), most experimental results confirm the positive impact of training on improving users' knowledge of cybersecurity.

Bada, Sasse and Nurse (2015) consider why campaigns to improve cybersecurity awareness fail. They conclude that simply conveying knowledge about good security practices is not sufficient. Knowledge and awareness of cyber risks are necessary but not sufficient for the safe behaviour of users online; such measures must be complemented by other impact strategies. Correctly answering questions that demonstrate knowledge about cybersecurity does not mean that a person is motivated to behave appropriately. Shillair and others (2005) note that every Internet user plays a role in maintaining the integrity of the entire network. They also emphasize that many Internet users do not consider cybersecurity to be their responsibility. Thus, they find that, in addition to educating consumers, people should be persuaded to take personal responsibility for protecting themselves on the network. Their study illustrates the interdependence among user knowledge, personal responsibility and education in encouraging cybersecurity behaviour.

Against this background which combines professional and private perspectives the following proposition was suggested:

(P1): Knowledge and awareness support the safe use of the Internet thereby reducing individuals' exposure to cyber risk.

The third stream of research focuses on several aspects of problems related to the unsafe behaviour of people on the Internet. This unsafe behaviour may lead individuals to incur financial losses thereby discouraging them from similar behaviour in the future. Employee behaviour that affects cybersecurity in an organization is discussed and customers or people who use Internet technology for private use are analysed separately. Cybersecurity behaviour at work is subject to established regulations and policies and in the event of noncompliance with the imposed rules employees are held accountable. In contrast home users choose the safety rules they will follow based on their awareness, knowledge and personal experience. Mashiane and Kritzinger (2018) note that knowledge and awareness of cybersecurity should be considered lower in the case of home users. Although there are different opportunities for education outside the workplace individuals do not have direct professional support and behaviour at home is different from that at work. Unlike employees in the workplace home users are not trained or protected by technical staff updating security software and hardware. An interesting observation has been provided by Kostyuk and Wayne (2021) saying that although experiencing personal data breach increases risk awareness actual online behaviour is difficult to change.

Mashiane and Kritzinger (2021) indicate that a home computer user's intention to perform cybersecurity-related behaviour is influenced by a combination of cognitive, social, and psychological components. Mamonov and Benbunan-Fich (2018) prove that awareness of information security threats

strengthens the power of newly selected passwords. The results indicate that an effective method of stimulating the use of strong passwords may be to embed a special message in the narrative, that is, introduce users to narratives that highlight cyber risk.

A report by McKinsey (2020) indicates that the role of the digital economy will increase in the years to come with strong pressure on CEE countries to digitalize their economies to improve labour efficiency. An increased role of digital solutions will probably be followed by an increased incidence of cyber attacks as noticed during the COVID-19 pandemic (Aldasoro et al., 2021). Therefore the number of "bad experiences" and losses incurred will also increase.

Against this background the second research proposition was formulated:

(P2): Individuals' experiences in the form of losses related to cyber risk support improvements in safe performance on the Internet.

2. Research methodology

To achieve the research goal a CAWI survey (computer-assisted web interview) was conducted in October 2020 among a sample of 1,804 Polish adult respondents who are Internet users. Sample weights were applied (Polish adult population divided by the number of survey respondents) to ensure representation. Moreover, the sample is chosen randomly. Surveys as a research method are commonly used to verify the behavioural aspect of economic and social mechanisms. As with many other research methods there are also some disadvantages of surveys. For instance, respondents may provide responses that are socially acceptable positive or in line with the popular opinion. These disadvantages can be to some extent minimized by using a large, representative research sample (the characteristics of the respondents are presented in Table A1 in the Appendix), which is the case in this study. Moreover, the time in which the respondent provides an answer is monitored and the least credible respondents are removed from the research sample.

The reliability of the results of this study is also confirmed by the repeatability of the conclusions. In 2021, the Polish Bank Association conducted a survey regarding cybersecurity on a sample of 1010 Polish citizens in which they asked questions very similar to those used here. Their results differ only slightly from those of this study (ZBP, 2021). However, this study is much broader and is complemented by a quantitative approach to investigate behavioural mechanisms.

Conducting the study during the coronavirus pandemic is an additional advantage as the role of remote work and Internet-based communication channels in this period jumped to a high level. Therefore, it is crucial to pay attention to the respondents' online behaviour during the pandemic. The size of the research sample is larger than that in most studies related to individuals' atti-

tudes towards cybersecurity (e.g., 459 responses in Zwilling and others (2020); 481 in Anwar and others (2017); 210 in Vance, Siponen and Pahnila (2012); 312 in Herath and Rao (2009)).

The survey questions operationalized the research propositions (P1 and P2). The first part of the survey concerned the verification of the **knowledge** of respondents about cybersecurity. To assess the level of knowledge five questions were asked. The list of questions and the correct answers are provided in Table A2 in the Appendix. Measuring users' knowledge of cybersecurity through a short quiz is also used by other researchers such as Zwilling and others (2020) or Chandarman and Van Niekerk (2017).

The first three questions concern password security, public Wi-Fi security and the difference between http and https. These three questions were also asked by Olmstead and Smith (2017) to a sample of 1,055 Americans in an online survey conducted in June 2016. Therefore it was possible to compare the knowledge of Americans with the knowledge of Poles in terms of these three questions.

In the next stage, the survey verified individuals' **awareness** of cyber risk by asking the respondents to organize operational risk events from most to least frequent in Europe. Among the operational risk events to be ordered by the respondent were cyber incidents, plane crashes, strong earthquakes, own house fire, winning an amount greater than PLN 1 million in a lottery and bank default. Placing cyber incidents in first place in the ranking translated into five points, second place four points and so forth. At the beginning of the questionnaire the respondents were provided with a definition of cyber risk.

In addition to knowledge and awareness, the respondents' **self-assessment** regarding cybersecurity on a scale from 1 (lack of knowledge) to 7 (high level of knowledge) was checked. Following Hosany and Martin (2012) self-assessed knowledge is considered a significant factor affecting consumer behaviour. This study took into account the respondents' **experiences** related to cyber risk. To this end, the following question was asked, "Have you ever suffered losses due to cyber risks?"; possible answers were "yes" or "no". The role of experience in consumer behaviour has been confirmed by many studies (e.g., Lusardi & Tufano, 2015 or Li, Xie & Zhang, 2020); therefore it is necessary to include this variable in this study. Descriptive statistics for the knowledge, awareness, self-assessment and experience variables are reported in Table A3 in the Appendix.

The main purpose of the survey was to verify individuals' **behaviour** in the cyber world (or network). For this purpose the respondents have to mark the behaviours they use to increase cybersecurity, broken down into two types: **general network behaviour** and **online banking behaviour**. In this the survey followed the questionnaire used by Zwilling and others (2020) (for general network behaviour) and the indications of the Polish Financial Supervisory Authority (for Internet banking behaviour). Table 1 presents the possible answers and the descriptive statistics are provided in Table A4 in the Appendix.

Table 1. Questions about behaviour on the network and Internet banking

General network behaviour: Which of the following tools are you using to mitigate cyber risk?		**Internet banking behaviour:** Which of the following tools are you using to mitigate cyber risk in Internet banking?	
Possible options	**Share of respondents (%)**	**Possible options**	**Share of respondents (%)**
Strong password	63.7	Strong password	60.8
Frequent password changes	33.2	Frequent password changes	25.6
I make sure that every software used on my computer is updated	41.1	I avoid using public computers to log into an Internet bank account	59.4
I create backups of my data	30.2	I avoid using open networks to log into an Internet bank account	56.1
I have installed and updated anti-virus software	62.7	I participate in training courses or read the information provided by the bank in the field of cybersecurity in Internet banking in detail	3.8
I have SPAM protection	24.9	I do not open suspicious links in received e-mail and SMS messages	66.8
I avoid using public computers	56.8	I have installed and updated anti-virus software	53.3
I avoid using open networks	49.8	I periodically check whether the account numbers in defined transfers have not been changed	28.8
I participate in training courses or learn about cybersecurity in detail	4.5	Before confirming the transaction, I verify the compliance of the account number to which I transfer funds with the recipient's number	48.8
I regularly review the security of computer data	24.4	I regularly review the account history and operations on each payment card for suspicious transactions	47.6
I avoid installing various types of applications from unknown sources	63.7	I do not copy bank account numbers for transfers ("copy-paste"), but I enter them myself and verify them thoroughly	32.6
		I make sure that all software used on my computer comes from a legal and trusted source	40.6
		I would immediately report any unusual or suspicious activities to the bank	42.5

Source: Own study.

The number of behaviours selected by a given respondent translates into the degree of safety of their online behaviour. The respondents were divided into those who showed a low level of safety (0 to 3 options), a medium level of safety (4 to 6 options) and a high level of safety (more than 6 options). The group selection considered their size so that no group accounted for less than 20% of the research sample. This division applies to both general network behaviour and Internet banking behaviour. In the case of Internet banking it was necessary to excluded 115 people who did not have an online account at a bank from the sample (i.e., 6.4% of respondents).

Ordinal logistic regression was applied where the dependent variable was respondent behaviour (1: low level of safety in behaviour; 2: medium level of safety; 3: high level of safety) and the explanatory variables were demographic characteristics (gender, age, income, place of residence) and experience (binary variable). To answer the research question the models were constructed separately for knowledge (assessed on a scale from 0 to 5), awareness (assessed on a scale from 0 to 5) and self-assessment (assessed on a scale from 1 to 7). Additionally, Lusardi and Tufano (2015), who analyse the role of debt literacy in the excessive indebtedness of respondents separately tested debt literacy variables and self-assessment using multinomial logistic regression. In addition, in this study the regression results were presented separately for general network behaviour and Internet banking behaviour. Variance inflation factor analysis confirmed the absence of collinearity of the variables.

In addition to the ordinal logistic model, a two-stage least-squares regression (2SLS) was used. On the one hand, the use of an additional type of regression provides a robustness check, but on the other it also presents the issues with the use of linear models to assess the impact of education variables (such as knowledge, awareness and self-assessment) on consumer behaviour. For the purposes of this study three variables (knowledge, awareness and self-assessment) are called **educational variables (EVs)**. The key factor influencing the choice of the 2SLS regression is that the education variables are endogenous. The knowledge, awareness and self-assessment variables may affect consumer behaviour but the direction of the impact may also be two-sided—consumers may also increase their knowledge, awareness and self-assessment as a result of their behaviour. In this case applying OLS will lead to simultaneity bias. The endogeneity problem can be illustrated by Equations (1) and (2):

$$Behaviour_i = \alpha_1 Controls_i + \beta_1 EV_i + \varepsilon_i \quad (1)$$

$$EV_i = \alpha_2 Controls_i + \beta_2 Behaviour_i + \varepsilon_i \quad (2)$$

where *Controls* include respondent *i*'s demographic variables (gender, age, income and place of residence) and experiences related to cyber risk. *Behaviour* in this case is understood as a number of options selected by a given respond-

ent to mitigate cyber risk (see Table 1). The first equation explains behaviour with the EVs. The second equation explains the EVs with behaviour. OLS regression will not distinguish between those equations. However, it is possible to find a proper instrument to determine the effect of the EVs on behaviour. Introduced endogeneity bias in educational research can be solved by using instrumental variable analysis (e.g., Watanapongvanich, Binnagan, Putthinun, Khan, & Kadoya, 2021).

The proper instrument used in regression constitutes a proxy for the EVs. At the same time this instrument (IV) has to be uncorrelated with the residuals from Equation (1). This proxy can be obtained via Equation (3), called a first-stage regression:

$$EV_i = \alpha Controls_i + \gamma IV_i + \varepsilon_i \tag{3}$$

In this equation the EVs are explained by *Controls* and *IV*. In the next stage EVs can be explained with the following Equation:

$$\overline{EV}_i = \overline{\alpha} Controls_i + \overline{\gamma} IV_i \tag{4}$$

where $\overline{\alpha}$ and $\overline{\gamma}$ are the estimated coefficients of Equation (3), i.e., the first-stage regression. $\overline{EV}_i$ is the estimated value of the EV. Note that if IV_i is uncorrelated with the residuals in Equation (1), $\overline{EV}_i$ will also be uncorrelated with the residuals. Finally the second-stage regression can be described as:

$$Behaviour_i = \alpha_3 Controls_i + \beta_{iv} \overline{EV}_i + \varepsilon_i \tag{5}$$

where β_{iv} is a casual effect of the EV on respondents' behaviour. This research separately assessed the causal effect of each EV (knowledge, awareness and self-assessment).

At this stage the key question arises: which instrument will be the most appropriate for the 2SLS regression? An appropriate instrument should have two features (Frijns, Gilbert, & Tourani-Rad, 2014). First, the instrument should correlate with an endogenous variable (here, with the EVs). Second, an instrument cannot be correlated with the residual in Equation (1). According to the literature, the most suitable instruments are, e.g., family background measured by financial situation or degree of the oldest sibling (Van Rooij, Lusardi & Alessie, 2011a), economic courses of the respondent (Van Rooij, Lusardi & Alessie, 2011b), and the participant's age (Dvorak & Hanley, 2010) or personality traits in terms of self-esteem (Mruk, 2006). In this research higher economic courses of the respondent was used as an instrument. According to the characteristics of Polish society, the respondent's higher education is significantly related to the parent's education (which is also a frequently used instrument in educational research) (Chłoń-Domińczak & Kotowska, 2015). Moreover,

economic education seems to be correlated with knowledge of cybersecurity (especially regarding Internet banking) but at the same time it should not be correlated with cybersecurity behaviour. The endogeneity issue and the weak instrument problem were tested by the Wu-Hausman test and *F*-statistics for the first-stage regression.

3. Results

According to the responses to the questions verifying cybersecurity knowledge Poles' knowledge about cybersecurity is average and comparable to the results presented by Olmstead and Smith (2017) for a sample of 1,055 respondents in the US (see Figure 1). Poles reported slightly better habits in two areas (i.e., password security and the difference between http and https) but slightly worse habits in the case of public Wi-Fi security. It is worth noting that while Polish respondents are able to identify a strong password as many as 38% of them admit that they use the same password for different web portals. One should note however limited comparability of survey data on cross-country basis.

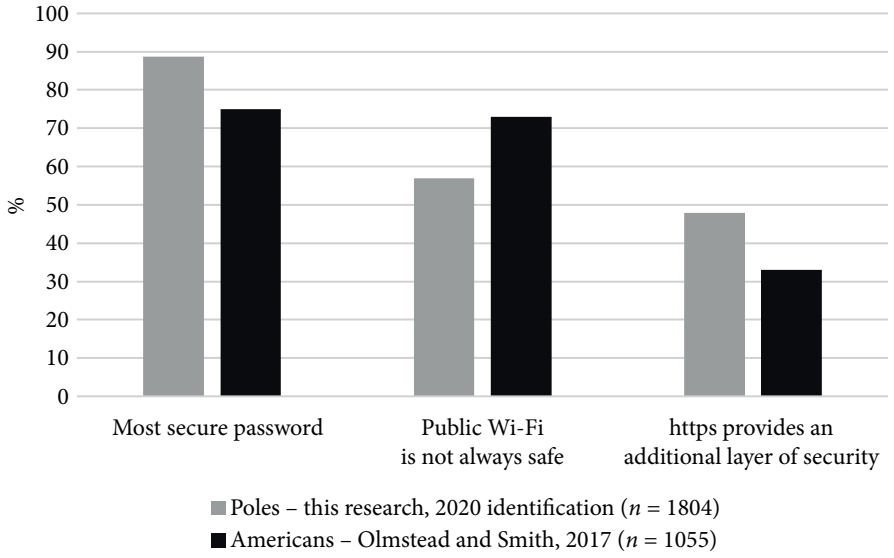

Figure 1. Percentage of correct answers to three questions verifying the respondent's cybersecurity knowledge

Note: There were slight differences between the content of the questions in this study and those in Olmstead and Smith (2017); however the questions addressed the same areas of knowledge. The percentages of correct answers to the remaining two questions asked in the survey are presented in Table A3 in the Appendix.

Source: Own study.

Table 2. The relationship between general network behaviour and knowledge, awareness and self-assessment

Reference variable	Variables	(1.1)	(2.1)	(3.1)
Female	Gender (male)	–0.0993 (0.0969)	–0.0479 (0.0955)	–0.1566 (0.0969)
Age 18–24	Age 25–44	–0.0262 (0.1401)	–0.2039 (0.1374)	–0.1864 (0.1377)
	Age 45–64	0.3496* (0.1436)	–0.0104 (0.1387)	0.1424 (0.1406)
	Age > 64	0.6462*** (0.1807)	0.4006* (0.1771)	0.4647** (0.1784)
Income < 1500	INC_1500_2499	0.0164 (0.1429)	0.1509 (0.1409)	0.0711 (0.1410)
	INC_2500_3499	–0.0680 (0.1423)	0.0596 (0.1401)	0.0162 (0.1408)
	INC_3500 _4499	0.0392 (0.1631)	0.2681 (0.1606)	0.1452 (0.1615)
	INC_higher_4499	0.3020 (0.1690)	0.5359*** (0.1664)	0.4206* (0.1673)
Village	Town to 100K	0.0357 (0.1161)	–0.0126 (0.1143)	–0.0117 (0.1146)
	Town 100K-500K	0.0903 (0.1311)	0.1271 (0.1294)	0.1189 (0.1298)
	Town higher 500K	0.3676** (0.1433)	0.3423* (0.1415)	0.3678** (0.1418)
Experience		–0.6022*** (0.1395)	–0.6728*** (0.1365)	–0.9038*** (0.1395)
Knowledge		0.5604*** (0.0415)		
Awareness			0.2829*** (0.0350)	
Self-assessment				0.3275*** (0.0343)
Sample		1804	1804	1804
Pseudo *R*-square		0.0698	0.0361	0.0429

Note: The table presents the results of ordinal logistic estimation for general network behaviour. The dependent variable is a variable with values 1, 2 or 3 depending on the number of options indicated by a given respondent which are used to increase cybersecurity in the network (out of eleven possible options presented in Table 1). The standard error is given in parentheses under the coefficient value. *, **, and *** denote statistical significance at $p < 0.05$, $p < 0.01$, and $p < 0.001$, respectively. The first model (1.1) contains the estimation results with the knowledge variable, the second (2.1) contains the estimation results with the awareness variable and the third (3.1) contains the estimation results with the self-assessment.

Source: Own study.

Table 3. The relationship between Internet banking behaviour and knowledge, awareness and self-assessment

Reference variable	Variables	(1.2)	(2.2)	(3.2)
Female	Gender (male)	–0.1271 (0.1010)	–0.0729 (0.0991)	–0.1387 (0.1005)
Age 18–24	Age 25–44	0.1278 (0.1458)	–0.0663 (0.1429)	–0.0705 (0.1422)
	Age 45–64	0.5338*** (0.1498)	0.1697 (0.1443)	0.2552 (0.1455)
	Age > 64	1.3091*** (0.2023)	1.0671*** (0.1981)	1.0341*** (0.1967)
Income < 1500	INC_1500_2499	–0.2008 (0.1503)	–0.0737 (0.1476)	–0.1231 (0.1470)
	INC_2500_3499	–0.1612 (0.1494)	–0.0375 (0.1468)	–0.0347 (0.1464)
	INC_3500 _4499	0.0250 (0.1696)	0.2664 (0.1668)	0.2179 (0.1669)
	INC_higher_4499	0.0495 (0.1771)	0.2857 (0.1732)	0.2434 (0.1734)
Village	Town to 100K	0.0568 (0.1203)	–0.0130 (0.1182)	0.0013 (0.1178)
	Town 100K-500K	0.1724 (0.1364)	0.1727 (0.1343)	0.1698 (0.1341)
	Town higher 500K	0.1643 (0.1491)	0.1506 (0.1464)	0.1859 (0.1460)
Experience		–0.7267*** (0.1431)	–0.8155*** (0.1398)	–0.9840*** (0.1419)
Knowledge		0.5661*** (0.0434)		
Awareness			0.2765*** (0.0353)	
Self-assessment				0.2170*** (0.0347)
Sample		1689	1689	1689
Pseudo *R*-square		0.0782	0.0451	0.0388

Note: The table presents the results of ordinal logistic estimation for Internet banking behaviour. The dependent variable is a variable with values 1, 2 or 3 depending on the number of options indicated by a given respondent which are used to increase cybersecurity in Internet banking (out of thirteen possible options presented in Table 1). The standard error is given in parentheses under the coefficient value. *, **, and *** denote statistical significance at $p < 0.05$, $p < 0.01$, and $p < 0.001$, respectively. The first model (1.2) contains the estimation results with the knowledge variable, the second (2.2) contains the estimation results with the awareness variable, and the third (3.2) contains the estimation results with the self-assessment.

Source: Own study.

Moreover almost half of the respondents correctly identified cyber incidents as the event occurring with the highest frequency among the options listed and the average self-assessment of knowledge about cybersecurity was 4.03 on a scale of 1 to 7.

In the next stage the study answers the question of whether knowledge, awareness and self-assessment influence behaviour in the cyber world. The ordinal logistic regression results are presented in Table 2 (for general behaviour on the Internet) and Table 3 (for behaviour in Internet banking).

As shown in Table 2 and Table 3, knowledge, awareness and self-assessment significantly affect cybersecurity behaviour in general and Internet banking specifically. The signs of the estimates are positive which indicates that greater knowledge, awareness and self-assessment increase safe behaviour in the cyber world. All of these factors increase the chance that a given respondent will be assigned to a group characterized by a higher cybersecurity approach. This chance is higher in the case of an increase in knowledge than in the case of an increase in awareness (higher value of the estimated parameter for knowledge than for awareness considering the same variable range). Thus the results provide support for Proposition 1 (P1) that knowledge and awareness of cyber risk improve cybersecurity behaviour. This applies to both general network and Internet banking behaviour. These results are consistent with a study by Kennison and Chan-Tin (2020) who confirm in a sample of 235 respondents the positive impact of self-reported knowledge on cybersecurity behaviour.

Surprisingly the older group of respondents (55 years and more) presented significantly better cybersecurity behaviour. This may be related to the fact that older people may not follow all technological novelties and are more cautious with online activities. Moreover due to having more life experience this group appears to be more aware of potential dangers and may have higher wealth. Cain, Edwards and Still (2018) confirm that older users are involved in safer online activities than younger users.

Cyber risk experience was also statistically significant. According to the survey, less than 14% of respondents had ever suffered losses related to cyber risk. This value is slightly higher than that reported by Zwilling and others (2020) in which only 9% of respondents had personal experience with cyber attacks. In the current study this variable had a significant negative value. Therefore, experiences related to cyber risk do not improve cybersecurity behaviour. In contrast, respondents who have suffered a cyber loss continue to behave in a way that exposes them to similar losses. This finding does not provide support for Proposition 2 (P2). Significance of experiences with negative sign is even not sensitive to the model specification. Cain and others (2018) also fail to confirm that experiences related to cyber risk positively affect cybersecurity behaviour. This phenomenon may be explained by attitudes towards risk taking: individuals with high risk acceptance and / or high self-confidence may be prone to riskier behaviour. However, this study is not focused on psychological

characteristics. Moreover, the counterintuitive results of the variable experience result from the discussion of the results of the study in the context of the broadly understood financial competences of consumers. Lusardi and Tufano (2015) in the field of financial literacy confirmed that consumer experiences with finances influence healthy financial behaviour but this is a different subject from cybersecurity. After a negative experience related to a cyber incident the respondent still probably lacks knowledge about the security rules, or their actual online behaviour is difficult to change (see, e.g., Kostyuk & Wayne, 2021). What is more, based on the survey results, only 4% of respondents read cyber risk information or warnings sent by banks to their customers. This finding is in line with conclusions by Krol, Moroz and Sasse (2012). Reading this kind of information may protect consumers against risk-taking behaviour but this tool actually plays no role in building a cyber risk culture among customers. General network behaviour and Internet banking behaviour are affected by the same variables in the same direction, with one exception. Cybersecurity behaviour in the Internet banking is not determined by the place of residence. In the case of general cybersecurity behaviour, residents of cities with more than 500,000 residents have demonstrated a greater degree of cybersecurity.

In the next step, the instrumental variable analysis was conducted to confirm all of the conclusions from the logistic regression analysis (see Table 4 and Table 5).

In the instrumental variable analysis (similar to the ordinal logistic regression) it was confirmed that knowledge, awareness and self-assessment significantly affect cybersecurity behaviour in general and in Internet banking. In addition, the older group of respondents presented significantly better cybersecurity behaviour. Experiences related to cyber risk do not improve cybersecurity behaviour. Additionally, in Table A5 in the Appendix instrumental variable (i.e., higher economic courses) coefficients in the first stage regression are presented.

In almost all models in Tables 4 and 5, the Wu-Hausman test confirms that knowledge, awareness and self-assessment are rightly considered endogenous variables. Endogeneity was not confirmed only in models 1.4. and 1.5. in Table 5. However, the *F*-statistics of the first-stage regression in all models indicate that instrumental variable (i.e., higher economic courses) is not weak.

Conclusions

The coronavirus pandemic has shifted a large part of individuals' activities to remote channels. In such an environment cybersecurity is a key factor in reducing users' exposure to losses related to cyber risk. Cybersecurity is also related to banks' sensitivity to cyber incidents. Customers who adhere to the basic principles of using online banking will be less exposed to cyber attacks which will translate into reduced losses for banks. The goal of the study was

Table 4. Instrumental variable analysis—second-stage regression results for general behaviour

Reference variable	Variables	(1.3)	(2.3)	(3.3)
Female	Gender (male)	–0.2784 (0.1554)	–0.0479 (0.0955)	–0.1566 (0.0969)
Age 18–24	Age 25–44	0.0103 (0.3523)	–0.2039 (0.1374)	–0.1864 (0.1377)
	Age 45–64	0.6927* (0.2803)	–0.0104 (0.1387)	0.1424 (0.1406)
	Age > 64	0.8880** (0.3368)	0.4006* (0.1771)	0.4647** (0.1784)
Income < 1500	INC_1500_2499	–0.5534 (0.3997)	0.1509 (0.1409)	0.0711 (0.1410)
	INC_2500_3499	–0.6238 (0.3606)	0.0596 (0.1401)	0.0162 (0.1408)
	INC_3500 _4499	–0.6017 (0.4041)	0.2681 (0.1606)	0.1452 (0.1615)
	INC_higher_4499	–0.3712 (0.4049)	0.5359*** (0.1664)	0.4206* (0.1673)
Village	Town to 100K	0.0097 (0.2242)	–0.0126 (0.1143)	–0.0117 (0.1146)
	Town 100K-500K	–0.2469 (0.2940)	0.1271 (0.1294)	0.1189 (0.1298)
	Town higher 500K	0.1085 (0.2877)	0.3423* (0.1415)	0.3678** (0.1418)
Experience		–0.4010* (0.1740)	–0.6728*** (0.1365)	–0.9038*** (0.1395)
Knowledge		1.6313*** (0.2497)		
Awareness			0.2829*** (0.0350)	
Self-assessment				0.3275*** (0.0343)
Sample		1804	1804	1804
Wu-Hausman		8.1403**		
F-statistic		42.8028***	0.0361	0.0429

Note: The table presents the results of second-stage regression for general network behaviour. The dependent variable is the number of options indicated by a given respondent that are used to mitigate cyber risk in the network (out of 11 possible options presented in Table 1). The standard error is given in parentheses under the coefficient value. *, **, and *** denote statistical significance at $p < 0.05$, $p < 0.01$, and $p < 0.001$, respectively. The first model (1.3) contains the estimation results with the knowledge variable, the second (2.3) contains the estimation results with the awareness variable, and the third (3.3) contains the estimation results with the self-assessment. Higher economic courses were used as an instrumental variable for knowledge, awareness and self-assessment separately.

Source: Own study.

Table 5. Instrumental variable analysis—second-stage regression results for Internet banking behaviour

Reference variable	Variables	(1.4)	(2.4)	(3.4)
Female	Gender (male)	–0.3884 (0.2018)	–0.3183 (0.2090)	–1.3819** (0.4761)
Age 18–24	Age 25–44	0.7380 (0.4636)	0.1692 (0.6200)	–0.9335 (10.026)
	Age 45–64	1.6043*** (0.3740)	0.6267 (0.6016)	0.4158 (0.7733)
	Age > 64	2.6252*** (0.4376)	2.1755*** (0.5542)	1.4383 (0.8357)
Income < 1500	INC_1500_2499	–0.3891 (0.5239)	–0.1246 (0.5134)	–1.4502 (0.9458)
	INC_2500_3499	–0.2963 (0.4798)	–0.0826 (0.4770)	–0.9923 (0.7923)
	INC_3500 _4499	–0.1922 (0.5309)	0.3822 (0.4655)	–0.9433 (0.8703)
	INC_higher_4499	–0.0710 (0.5295)	0.5103 (0.4652)	–0.8009 (0.8608)
Village	Town to 100K	0.2810 (0.2832)	–0.0207 (0.3608)	–0.6200 (0.5736)
	Town 100K-500K	0.1302 (0.3567)	0.0170 (0.4070)	–0.7534 (0.6701)
	Town higher 500K	0.3797 (0.3572)	0.0907 (0.4385)	–0.5094 (0.6646)
Experience		–0.8023*** (0.2182)	–1.1061*** (0.2462)	–2.8054*** (0.6108)
Knowledge		1.5744*** (0.3278)		
Awareness			1.3420*** (0.3024)	
Self-assessment				2.1288*** (0.5741)
Sample		1689	1689	1689
Wu-Hausman		1.0207	2.8505	7.3884**
F-statistic		36.8986***	35.6949***	14.9003***

Note: The table presents the results of the second-stage regression for Internet banking behaviour. The dependent variable is the number of options indicated by a given respondent that are used to mitigate cyber risk in Internet banking (out of 13 possible options presented in Table 1). The standard error is given in parentheses under the coefficient value. *, **, and *** denote statistical significance at $p < 0.05$, $p < 0.01$, and $p < 0.001$, respectively. The first model (1.4) contains the estimation results with the knowledge variable, the second (2.4) contains the estimation results with the awareness variable, and the third (3.4) contains the estimation results with the self-assessment. Higher economic courses were used as an instrumental variable for knowledge, awareness and self-assessment separately.

Source: Own study.

to assess whether knowledge about cybersecurity and awareness of cyber risk can contribute to improving cybersecurity behaviour. The study investigated also the role of cyber risk losses in improving behaviour in the cyber world.

This research is important for several reasons. First, it evaluates knowledge and awareness of cybersecurity in Polish society. Because similar questions have also been asked in the US it is possible to compare the results between these two countries. Second, the results confirm avenues for reducing cyber risk, i.e., investing in society's knowledge of cyber issues. According to the ESRB (2018), the threat of cyber attacks may be related to systemic risk; therefore it is important to identify mechanisms to reduce such risk. Third the study is important for all Internet users to understand the determinants of cybersecurity.

To achieve the goal of this study a survey was conducted on a representative sample of 1,804 Polish citizens in October 2020. In the first stage of the survey the level of knowledge about cybersecurity, awareness of cyber risk and self-assessment in the area of cybersecurity were assessed. In the second stage the respondents' network behaviour, broken down into general network behaviour and Internet banking behaviour, was investigated. Verification was based on questions about the activities individuals use to reduce cyber risk. The more actions the respondent uses to mitigate cyber risk the safer his or her online behaviour. Based on their responses the respondents were classified into three groups, i.e., low, middle and high levels of cybersecurity behaviour.

The results of the ordinal logistic regression and the instrumental variable analysis indicate that higher knowledge, awareness and self-assessment significantly increase cybersecurity behaviour. This is true in the contexts of both general network behaviour and Internet banking activity. These results are robust to the method used to analyse the data and support research Proposition 1 (P1). The analyses also show that older people are more cautious about using the Internet. Experiencing losses related to cyber risk in the past did not change the behaviour of a given respondent. The key variable to improve cyber risk culture is knowledge and awareness of such risk rather than bad experiences. These conclusions do not support research Proposition 2 (P2), so not "every knock is a boost" which is in line with Kostyuk and Wayne (2021).

The analysis makes an important contribution to the discussion of the role of economic and financial education in consumer behaviour. The literature commonly confirms a positive impact of financial literacy on pension savings, the level of indebtedness, optimal savings decisions and general welfare. This research adds another element to the role of financial education, i.e., the positive impact of knowledge and awareness of cybersecurity. The study shows that only 4% of respondents read messages sent by banks on cybersecurity. Therefore, in future it is worth investigating how consumers prefer to gain knowledge about cybersecurity, the most efficient way to provide knowledge (Bada et al., 2015) and the expected role of financial services providers in this regard. Simply providing individuals with information or warnings is not sufficient to stimulate

safe behaviour. As Wogalter and others (2012) note, one cannot use the "average" consumer approach because it is necessary to reach those who are "below average". It can be argued that it is necessary to use approaches tailored to the needs of various groups of customers.

This study is not free of limitations. It did not analyse psychological characteristics related to risk-taking behaviour. Such an approach may be used in the future in behavioural finance studies or psychological studies.

Appendix

Table A1. Respondent profile

Variable	Share (%)
Gender	
Male	44.3
Female	55.7
Age	
18–24	16.4
25–44	38.0
45–64	34.8
Age > 64	10.8
Degree	
Elementary	8.6
Vocational	21.1
Secondary	39.9
Higher (economic studies)	7.6
Higher (non-economic studies)	22.8
Income (PLN)	
< 1500	19.8
1500–2499	23.0
2500–3499	27.2
3500–4499	15.6
> 4499	14.4
Place of residence	
Village	32.8
Town < 100,000 citizens	31.3
Town 100,000–500,000 citizens	20.5
Town > 500,000 citizens	15.4

Source: Own study.

Table A2. Cyber risk knowledge questions

Question	Possible answers
Q1. Which password is the most secure?	a) Łódź123 b) WTh!5Z c) Maria*48 d) Do not know
Q2. If a public Wi-Fi network (e.g., in a coffee shop or airport) requires a password, is it safe for activities such as electronic banking?	a) No, it is not safe b) Yes, it is safe c) Do not know
Q3. What is the difference between https and http protocols?	a) https provides an additional layer of security compared to http, as it uses the appropriate certificate to transfer the data. b) http is more secure than https as its operation is monitored by an antivirus program. c) http is not available for some users d) Do not know
Q4. Which activity is related to cyber risk?	a) Inability to purchase new computer software b) Theft of an ID card and taking a loan at a bank branch on this basis c) Publication of offensive content on the web d) Do not know
Q5. Which group of words are the names of antivirus programs?	a) Norton, McAfee, Avast b) Word, Excel, PowerPoint c) pdf, xls, doc d) Do not know

Source: Own study.

Table A3. Cyber risk questions (share of correct answers), awareness and self-assessment—descriptive statistics

Variable	Q1 (%)	Q2 (%)	Q3 (%)	Q4 (%)	Q5 (%)	Awareness	Self-assessment
Gender							
Male	80.78	55.48	40.44	30.48	87.25	4.07	4.19
Female	80.00	58.88	57.25	28.88	90.38	3.88	3.59
Age							
18–24	90.88	56.42	52.70	42.23	93.92	4.10	4.05
25–44	81.91	56.80	49.94	33,37	87.41	3.95	4.05
45–64	74.72	56.12	42.93	22,57	86.49	3.96	3.61
Age > 64	77.84	61.34	49.48	21.65	91.75	3.82	3.66
Degree							
Elementary	78.06	50.32	44.52	32.90	82.58	3.92	3.56
Vocational	72.70	46.19	31.76	24.93	79.53	3.65	3.46
Secondary	81.11	60.28	49.03	28.75	91.53	3.94	3.95
Higher (economic studies)	79.56	57.66	64.23	32.85	90.51	4.06	4.49
Higher (non-economic studies)	87.59	63.50	56.69	33.82	93.67	4.28	3.96
Income (PLN)							
< 1500	76.26	47.77	43.58	32.40	86.03	3.96	3.64
1500–2499	79.76	57.35	44.10	29.64	86.27	3.86	3.76
2500–3499	81.02	57.35	45.10	26.94	89.18	3.98	3.80
3500–4499	82.92	59.07	58.01	28.83	90.75	3.96	4.08
> 4499	83.46	66.15	54.23	32.69	92.69	4.12	4.19
Place of residence							
Village	79.73	57.09	43.07	32.77	85.81	3.86	3.72
Town < 100,000 citizens	77.88	51.68	47.79	26.19	87.79	3.92	3.82
Town 100,000–500,000 citizens	84.55	61.52	51.76	29.27	94.04	4.05	3.98
Town > 500,000 citizens	81.65	61.51	53.24	31.29	89.21	4.16	4.06

Note: Q1, Q2, Q3, Q4, Q5: share of correct answers to the questions presented in Table A2. Awareness: This variable represents the ordering of events by the respondent from the most frequent to the least frequent in Europe. Among the events that should be ordered by a respondent were cyber incidents, plane crash, strong earthquake, own house fire, winning an amount greater than PLN 1 million in a lottery, and bank default. Placing cyber incident in first place in the ranking meant receiving 5 points, second place, 4 points and so forth. Self-assessment: subjective assessment of cybersecurity knowledge on a scale from 1 (no knowledge) to 7 (high level of knowledge).

Source: Own study.

Table A4. Individuals' cybersecurity behaviour (average number of selected options)—descriptive statistics

Variable	General network behaviour	Internet banking behaviour
Gender		
Male	4.63	5.65
Female	4.49	5.68
Age		
18–24	4.45	5.18
25–44	4.36	5.29
45–64	4.63	5.83
Age > 64	5.15	6.97
Degree		
Elementary	4.36	5.13
Vocational	3.9	4.80
Secondary	4.59	5.91
Higher (economic studies)	4.91	5.58
Higher (non-economic studies)	5.05	6.19
Income (PLN)		
< 1500	4.32	5.43
1500–2499	4.51	5.49
2500–3499	4.41	5.58
3500–4499	4.67	5.86
> 4499	5.08	6.20
Place of residence		
Village	4.32	5.40
Town < 100,000 citizens	4.49	5.62
Town 100,000–500,000 citizens	4.71	5.87
Town > 500,000 citizens	4.96	6.03

Note: General network behaviour: the average number of actions (according to Table 1) indicated by the respondent to reduce risk on the network (11 options available to choose from). Internet banking behaviour – the average number of actions (according to Table 1) to reduce risk in online banking (13 options to choose from).

Source: Own study.

Table A5. Instrumental variable coefficients in the first stage regression

Dependent variable	General network behaviour			Internet banking behaviour		
	knowledge	awareness	self--assessment	knowledge	awareness	self--assessment
Higher economic courses	0.5439*** (0.0831)	0.6352*** (0.0997)	0.4293*** (0.0967)	0.5119*** (0.0842)	0.6005*** (0.1005)	0.3786*** (0.0651)

Note: The table presents the instrumental variable coefficients in the first-stage regression. Due to different sample size, instrumental variable coefficients are different for general network and Internet banking behaviour. The standard error is given in parentheses under the coefficient value. *, **, and *** denote statistical significance at $p < 0.05$, $p < 0.01$, and $p < 0.001$, respectively.

Source: Own study.

References

Aldasoro, I., Frost, J., Gambacorta, L., & Whyte, D. (2021, January). Covid-19 and cyber risk in the financial sector. *BIS Bulletin*, *37*, 1–9.

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.

Association of Certified Fraud Examiners. (2020, December). *Fraud in the wake of COVID-19: Benchmarking report*.

Bada, M., Sasse, A. M., & Nurse, J.R.C. (2015). *Cyber security awareness campaigns: Why do they fail to change behaviour?*. (Paper presented at the 1st International Conference on Cyber Security for Sustainable Society). *Sustainable Society Network*, 118–131.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. *European Journal of Information Systems*, *18*(2), 151–164.

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, *42*, 36–45.

Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *The African Journal of Information and Communication*, *20*, 133–155.

Chłoń-Domińczak, A., & Kotowska, I. E. (Eds.). (2015). *Uwarunkowania decyzji edukacyjnych*. Warszawa: Instytut Badań Edukacyjnych.

Da Veiga, A. (2018). An approach to information security culture change combining ADKAR and the ISCA questionnaire to aid transition to the desired culture. *Information & Computer Security*, *26*(5), 584–612.

Dvorak, T., & Hanley, H. (2010). Financial literacy and the design of retirement plans. *The Journal of Socio-Economics*, *39*(6), 645–652.

ESRB. (2018). Press release: *The general board of the European Systemic Risk Board held its 32nd regular meeting on 6 Dec 2018*.

Frijns, B., Gilbert, A., & Tourani-Rad, A. (2014). Learning by doing: The role of financial experience in financial literacy. *Journal of Public Policy*, *34*(1), 123–154.

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2020). A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems*, 1–11.

Grazioli, S., & Wang, A. (2001). *Looking without seeing: Understanding unsophisticated consumers' success and failure to detect Internet deception*. (ICIS 2001 Proceedings, 193–203).

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125.

Hosany, S., & Martin, D. (2012). Self-image congruence in consumer behavior. *Journal of Business Research*, *65*(5), 685–691.

Hughes-Larteya, K., Li, M., Botchey, F. E., & Qin, Z. (2021). Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon*, *7*(3), 1–13.

Hussain, A., Mohamed, A., & Razali, S. (2020). *A review on cybersecurity: Challenges & emerging threats*. (NISS2020: Proceedings of the 3rd International Conference on Networking, Information Systems & Security No. 28, 1–7).

Junger, M., Montoya, & L., Overink, F.-J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior*, *66*, 75–87.

Kennison, S. M., & Chan-Tin, E. (2020). Taking risks with cybersecurity: Using knowledge and personal characteristics to predict self-reported cybersecurity behaviors. *Frontiers in Psychology*, *11*, 1–9.

Kostyuk, N., & Wayne, C. (2021). The microfoundations of state cybersecurity: Cyber risk perceptions and the mass public. *Journal of Global Security Studies*, *6*(2), 1–25.

Kosub, T. (2015). Components and challenges of integrated cyber risk management. *Zeitschrift für die gesamte Versicherungswissenschaft*, *104*, 615–634.

Krol, K., Moroz, M., & Sasse, M. A. (2012). *Don't work. Can't work? Why it's time to rethink security warnings*. (Paper presented at the 7th International Conference on Risk and Security of Internet and Systems (CRiSIS), 1–8).

Li, H., Xie, K. L., & Zhang, Z. (2020). The effects of consumer experience and disconfirmation on the timing of online review: Field evidence from the restaurant business. *International Journal of Hospitality Management*, *84*, 1–11.

Lis, P., & Mendel, J. (2019). Cyberattacks on critical infrastructure: An economic perspective. *Economics and Business Review*, *5*(2), 24–47.

Lusardi, A., & Tufano, P. (2015). Debt literacy, financial experiences, and overindebtedness. *Journal of Pension Economics and Finance*, *14*(4), 332–368.

Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, *83*, 32–44.

Mashiane, T., & Kritzinger, E. (2018). Cybersecurity behaviour: A conceptual taxonomy. In: O. Blazy, C. Y. Yeun (Eds.), *Information security. Theory and practice*. (12th IFIP WG 11.2 International Conference, WISTP, 147–156).

Mashiane, T., & Kritzinger, E. (2021). Identifying behavioral constructs in relation to user cybersecurity behavior. *Eurasian Journal of Social Sciences*, *9*(2), 98–122.

McKinsey. (2020). *Digital challengers in the next normal in Central and Eastern Europe on a path to digitally-led growth*. McKinsey Digital.

Milošević, N., Dobrota, M., & Barjaktarović Rakočević, S. (2018). Digital economy in Europe: Evaluation of countries' performances. *Proceedings of Rijeka Faculty of Economics: Journal of Economics and Business*, *36*(2), 861–880.

Mruk, C. J. (2006). *Self-esteem research, theory, and practice: Toward a positive psychology of self-esteem*. New York: Springer Publishing Company.

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*, *29*(3), 306–321.

Olmstead, K., & Smith, A. (2017, March 22). What the public knows about cybersecurity. *Pew Research Center*.

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making*, *9*(2), 117–129.

Reegård, K., Blackett, C., & Katta, V. (2019). *The concept of cybersecurity culture*. (Paper presented on the 29th European Safety and Reliability Conference).

Shillair, R., Cotton, S. R., Tsai, H.-Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2005). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, *48*, 199–207.

Tedder, K. (2020). *The escalation of digital fraud: Global impact of the coronavirus.* Report by Javelin Strategy & Research and SAS.

Van Rooij, M., Lusardi, A., & Alessie, R. (2011a). Financial literacy and stock market participation. *Journal of Financial Economics*, *101*(2), 449-–472.

Van Rooij, M., Lusardi, A., & Alessie, R. (2011b). Financial literacy and retirement planning in the Netherlands. *Journal of Economic Psychology*, *32*(4), 593–608.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3), 190–198.

Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. (2019). Cyber security education is as essential as "the three R's". *Heliyon*, *5*(12), 1–8.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102.

Watanapongvanich, S., Binnagan, P., Putthinun, P., Khan, M. S. R., & Kadoya, Y. (2021). Financial literacy and gambling behavior: Evidence from Japan. *Journal of Gambling Studies*, *37*(3), 445–465.

Wogalter, M. S., Laughery, Sr. K. R., & Mayhorn, C. B. (2012). Warnings and hazard communications. In: G. Salvendy (Ed.), *Handbook of human factors and ergonomics* (4 ed., pp. 868–894). Hoboken, NJ: John Wiley & Sons.

Yasin, A., Liu, L., Li, T., Wang, J., & Zowghi, D. (2018). Design and preliminary evaluation of a cyber Security Requirements Education Game (SREG). *Information and Software Technology*, *95*, 179–200.

Yildirim, M., & Mackie, I. (2019). Encouraging users to improve password security and memorability. *International Journal of Information Security*, *18*, 741–759.

Związek Banków Polskich (ZBP). (2021). *Postawy Polaków wobec cyberbezpieczeństwa. Badanie Warszawskiego Instytutu Bankowości zrealizowane w ramach projek-*

tu Bezpieczeństwo w Cyberprzestrzeni. Retrieved from https://zbp.pl/getmedia/65f267e4-3316-4198-9cce-411d8f03de32/Postawy_Polakow_wobec_Cyberbezpieczenstwa_v-3

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 1–16.