The Influence of Organizational, Social and Personal Factors on Cybersecurity Awareness and Behavior of Home Computer Users

Joëlle Simonet and Stephanie Teufel(✉)

International Institute of Management in Technology (IIMT),
University of Fribourg, 1700 Fribourg, Switzerland
{joelle.simonet,stephanie.teufel}@unifr.ch

Abstract. With the increased use of computers and network systems in a time of digitalization, the digital connectedness frames our daily life at work and at home. To ensure secure systems, all computer users should safely interact with these systems. Prior research indicates insufficient cybersecurity awareness of home computer users who are also difficult to reach as they are not necessarily part of organizational structures. This study therefore investigates organizational, social and personal determinants of an individual's cybersecurity awareness and its influence on cybersecurity behavior in the home environment, using partial least squares structural equation modeling based on survey data. The results show a low influence of the workplace and weak social influences, while the study confirms a significant effect of personal initiative and a strong effect of information systems knowledge on an individual's cybersecurity awareness. The results suggest that security strategies aimed at the general public should focus on improving the knowledge and understanding instead of making fear. The study provides valuable insights about cybersecurity awareness and its determinants contributing to the field of research. The findings can be used for reviewing cybersecurity strategies.

Keywords: Cybersecurity awareness · Cybersecurity behavior · Home computer user

1 Introduction

The trends of digitalization and increased interconnectedness have reached most areas of the daily life. These trends enhance the risk of cyber threats such as cybercrime or system failure. Computer users' interactions with such systems are critical to preserving a safe cyber environment as many of them do not possess a deep understanding of computers or cyber threats [2,27,31,39]. While the

Published by Springer Nature Switzerland AG 2019
G. Dhillon et al. (Eds.): SEC 2019, IFIP AICT 562, pp. 194–208, 2019.
https://doi.org/10.1007/978-3-030-22312-0_14

management of cybersecurity has started in businesses, home users are often not aware of their responsibility [14,41]. Additionally, it demands the user's initiative to act secure [2,29]. The loosening of structures and decentralization, for example in smart grids [21] or with mobile working [7], call for safe user behavior in the home environment. Many studies have been conducted in the work context [7,12,18,25,33,38], the home user though has not received the same attention in research. Therefore, the present study aims to understand what factors influence a user's decision making for a safe (or unsafe) cyber behavior and to grasp what sources of information impact a computer user's cybersecurity awareness in his home environment.

The next section presents the theoretical background and the research model developed. In Sect. 3, the methodology used is presented, while the results of the analysis are listed in Sect. 4. A discussion of the findings (Sect. 5) and a conclusion (Sect. 6) round off this paper.

2 Theoretical Background and Research Model

A home computer user can learn about cybersecurity from various sources. The workplace of a user can function as a source by providing knowledge that the user might transfer to his home environment. Many organizations distribute security policies [18,25] or provide security training and awareness programs [12,18,41] explaining the correct use and interaction with computers and systems connected to the Web covering topics such as password management or phishing. Two streams differentiate how such security measures are implemented. While some authors suggest following the deterrence approach by creating fear-based campaigns [12,22], other researchers call for skills-based measures [18,24,39]. An all-encompassing approach towards cybersecurity in organizations is the promotion of an information security culture. According to [37], an information security culture should change employees' values in order to promote an intrinsic motivation for safe cyber behavior. As an intangible concept, information security culture has an impact on security awareness [34] but is in return nurtured through awareness [11,38]. In line with this, it is assumed that policy provision, security training and an information security culture at the workplace influence the cybersecurity awareness of a home computer user. The corresponding hypotheses are:

> H1a: *Information Security Policy Provision (ISPP)* in the individual's workplace is positively related to the individual's *Cybersecurity Awareness (CSA).*

> H1b: *Security Training and Awareness Programs (SETA)* in the individual's workplace is positively related to the individual's *Cybersecurity Awareness.*

> H1c: *Information Security Culture (ISC)* in the individual's workplace is positively related to the individual's *Cybersecurity Awareness.*

More informal determinants of a user's cybersecurity awareness can be found in the social environment of a home computer user. Especially since consequences of cybersecurity incidents are not always visible directly or at anytime, stories told by friends and family can act as vicarious examples and enhance a social learning process for cybersecurity issues [5,23,31].

International guidelines such as from the OECD [30] or national cybersecurity strategies target the society and thus include home computer users. It remains difficult though to reach out to those who are in loosely coupled structures [43]. Information provided by the public administration or reports distributed by the mass media can highlight the importance of cybersecurity and deliver security advice [18,29,31].

> H2a: *Family and Friends Influence (FFI)* is positively related to the individual's *Cybersecurity Awareness.*

> H2b: *Mass Media Influence (MMI)* is positively related to the individual's *Cybersecurity Awareness.*

> H2c: *Public Administration Information (PAI)* is positively related to the individual's *Cybersecurity Awareness.*

Compared to the work environment, a home user is required to be self-initiative to learn about cybersecurity topics and take security-enhancing actions [2,29,39]. Being someone generally showing personal initiative is thus assumed to have a positive effect on awareness. In this context, having previous information systems knowledge is expected to be a strong determinant of cybersecurity awareness [14,18,31].

> H3a: *Personal Initiative (PI)* is positively related to the individual's *Cybersecurity Awareness.*

> H3b: *Information Systems Knowledge (ISK)* is positively related to the individual's *Cybersecurity Awareness.*

Understanding an individual's behavior or the factors influencing a decision to act are hard to grasp. Behavioral models such as the *Theory of Planned Behavior* [1] or the *Protection Motivation Theory* [35,36] have been developed to investigate the cognitive processes involved. In the *Protection Motivation Theory*, the threat appraisal and the coping appraisal represent the two sides of the mediating process of an individual's intention to protect something (or someone) from a threat [36,44]. Originally used for investigating health-related fears, the components of the model have been used to study cybersecurity fears many times [2,17,28,39,45]. Perceived vulnerability and perceived severity are elements of the threat appraisal, while perceived self-efficacy, perceived response efficacy and perceived costs constitute the coping appraisal. In the context of cybersecurity, the elements represent the understanding of a threat and the mental process an individual goes through before deciding to behave securely or not and therefore represent the construct of cybersecurity awareness (H5a-e).

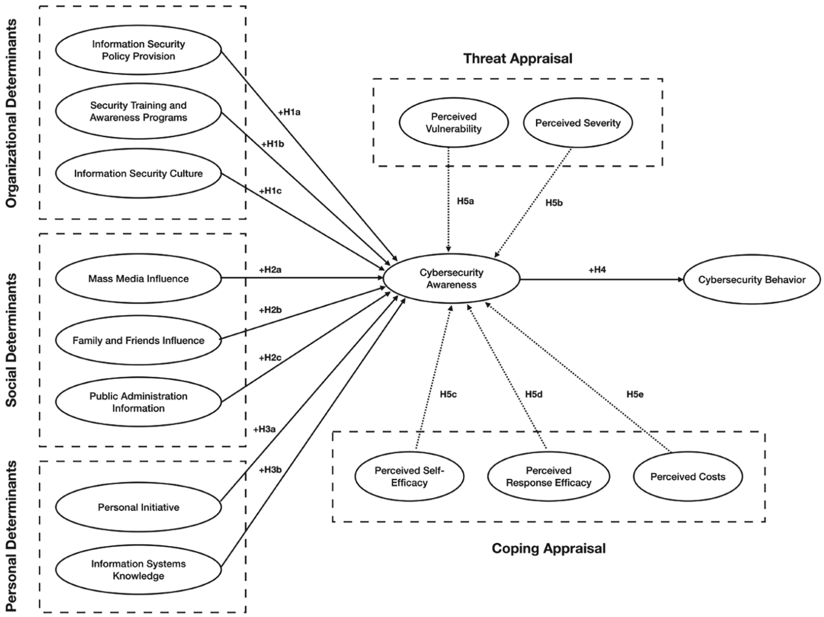

Fig. 1. Research model

H4: *Cybersecurity Awareness* is positively related to the individual's *Cybersecurity Behavior (CSB)*.

Figure 1 shows the research model summarizing the organizational, social and personal determinants, the multi-dimensional construct of cybersecurity awareness and cybersecurity behavior (for details, see [40]).

3 Methodology

This study draws on common methods in the domain of cybersecurity awareness and behavior research [2,18,29,39]. For the data collection, a survey was conducted, while the data analysis was performed with partial least squares structural equation modeling. Details about the analysis are given in Sect. 4.

The data collection process encompassed a self-report online questionnaire that was implemented via SoSci Survey, a Germany-based web tool for conducting online questionnaires [26]. Although using self-reported data can provoke a social desirability bias [8,9], it allows to capture the respondents' cognitive process [4] which was essential for this study. By allowing an anonymous completion of the questionnaire for which the respondent was not required to leave his familiar environment, the risk for social desirability bias was reduced [8].

The survey was sent out to employees of various organizations in Switzerland. This mode of distribution was chosen to ensure that participants work, which was necessary for being able to investigate the influence of the workplace. Organizations contacted are located in the French-, German- and Italian-speaking parts of Switzerland and are active in areas such as educational, health and social, IT-related businesses or public transport. The questionnaire was made available in German, English and French.

After a data collection of about five weeks, a total number of 562 participants started the questionnaire. Removing the unfinished cases and the records with more than 15% of missing data, suspicious response patterns and outliers as suggested by [16] results in 456 cases used for further analysis. Mean-value replacement is applied for the remaining missing data. Table 1 shows some demographic characteristics of the participants. A more detailed discussion of the sample can be found in [40].

Table 1. Demographic characteristics of the participants

Demographics	**n**	**%**		**n**	**%**
Sex			*Total*	*456*	*100*
Female	224	49.1			
Male	227	49.8	**Linguistic Region**		
Age			German-speaking	116	25.4
under 18	5	1.1	French-speaking	327	71.7
18-24	34	7.5	Italian-speaking	6	1.3
25-34	131	28.7	other / not CH	7	1.5
35-44	101	22.1	**Sector**		
45-54	109	23.9	Public Sector	410	89.9
55-64	72	15.8	Private Sector	25	5.5
over 64	3	0.7	Voluntary Sector	15	3.3

The survey is organized in eight sections covering the personal, social and organizational determinants, the variables constituting cybersecurity awareness, the construct of cybersecurity behavior as well as additional demographic questions such as age, gender or language region. This results in a total number of 53 items, all constructed as closed questions, corresponding to statements to which respondents indicate their level of agreement on a 5-point Likert scale. For three items, different minimum and maximum values are used.

The measures for the fourteen constructs are all adapted from previously validated constructs. A pretest was conducted to ensure the comprehensibility of the questionnaire. Some items were reworded and others exchanged before being subject of a second pretest. A general approach on cybersecurity actions was chosen to get an all-encompassing point of view and to avoid technology dependency and thus facilitate the repeatability of the study.

Information Security Culture, *Friends and Family Influence*, *Information Systems Knowledge* are considered reflective. The remaining constructs, *Information Security Policy Provision*, *Security Training and Awareness Programs*, *Mass Media Influence*, *Public Administration Information*, *Personal Initiative* as well as *Cybersecurity Behavior* are considered formative. *Cybersecurity Awareness* is constructed as a reflective-formative second-order construct composed of the first-order constructs *Perceived Vulnerability*, *Perceived Severity*, *Perceived Self-Efficacy*, *Perceived Response Efficacy* and *Perceived Costs*. All constructs and the corresponding items in their final version can be found in Table 5 in the Appendix.

4 Analysis and Results

The model was analyzed with partial least squares structural equation modeling using the software SmartPLS 3.2.5 [32]. The analysis encompasses a first step of assessing the measurement models and a second step of evaluating the structural model. The analysis was conducted by following the guidelines proposed by [15] and [16]. For significance testing, 5000 bootstrap samples were used. Additionally, a mediation analysis was performed to investigate the awareness' mediating role.

4.1 Measurement Model Assessment

The proposed research model includes formative and reflective constructs, which require a different assessment. For reflective constructs, internal consistency and indicator reliability and the average variance extracted (AVE) are used to verify convergent validity. A composite reliability (CR) value between 0.7 and 0.9 indicates internal consistency reliability, higher values suggest high item similarity [16]. For the AVE, values above 0.5 are desired. Indicator reliability is assessed with the outer loading (OL) of the items, which indicate the strength of the path and should exhibit values above 0.7. Items with an outer loading between 0.4 and 0.7 can be kept in the model, while indicators with a lower loading should be removed [16]. All values are in the accepted ranges, except for *Information Systems Knowledge* that exhibits values above the desired values (see Table 2). Discriminant validity is assessed with the HTMT criterion as suggested by [15,19]. As all values are below 0.85, discriminant validity is established between all latent variables (see Table 3)

Formative constructs are assessed by looking at the variance inflation factor (VIF) for collinearity issues and the relative importance of each indicator. VIF values should be below five for all indicators. The items should exhibit significant outer weight or, if not, manifest outer loadings above 0.5. Indicators should be removed if neither the outer loading nor the outer weight is significant. The values are shown in Table 2. The items MMI3 and PAI3 were removed for further analyses. The reflective-formative second-order construct *Cybersecurity Awareness* is evaluated in the same manner.

Table 2. Reflective and formative constructs

Reflective				Formative							
Item	OL	CR	AVE	Item	VIF	Outer weight			Outer loading		
	l					w	t	p	l	t	p
ISC1	0.728	0.799	0.507	ISPP1	2.187	0.258	1.288	0.198	0.843*	8.413	0.000
ISC2	0.476			ISPP2	2.187	0.794*	3.586	0.000	0.985*	26.356	0.000
ISC3	0.77			SETA1	1.871	0.722*	2.081	0.037	0.965*	7.834	0.000
ISC4	0.825			SETA2	1.871	0.356	1.154	0.249	0.849*	4.508	0.000
FFI1	0.758	0.895	0.682	MMI1	1.503	0.344	1.278	0.201	0.732*	3.337	0.001
FFI2	0.853			MMI2	1.791	0.885*	2.786	0.005	0.863*	4.706	0.000
FFI3	0.821			MMI3^r	1.280	−0.471	1.889	0.059	0.033	0.201	0.841
FFI4	0.867			PAI1	1.752	0.914*	4.790	0.000	0.976*	18.604	0.000
ISK1	0.954	0.955	0.914	PAI2	2.230	0.202	0.992	0.321	0.665*	4.350	0.000
ISK2	0.957			PAI3^r	1.390	−0.251	1.555	0.120	0.105	0.883	0.377
PV1	0.83	0.874	0.698	PI1	1.826	0.353*	2.040	0.041	0.782*	8.640	0.000
PV2	0.833			PI2	1.891	0.538*	2.866	0.004	0.833*	10.476	0.000
PV3	0.844			PI3	1.629	0.460*	2.798	0.005	0.775*	8.175	0.000
PS1	0.708	0.864	0.682	PI4	1.366	−0.376*	2.487	0.013	0.214	1.696	0.090
PS2	0.929			PV	1.069	−0.007	0.243	0.808	−0.136*	2.034	0.042
PS3	0.825			PS	1.060	0.047	1.155	0.248	0.161*	2.217	0.027
PSE1	0.817	0.899	0.691	PSE	1.645	0.747*	12.019	0.000	0.952*	49.290	0.000
PSE2	0.833			PRE	1.305	0.310*	5.053	0.000	0.674	12.690	0.000
PSE3	0.852			PC	1.355	−0.125*	2.063	0.039	−0.570	10.116	0.000
PSE4	0.822			CSB1	1.312	0.225*	3.003	0.003	0.564*	7.955	0.000
PRE1	0.566	0.825	0.546	CSB2	1.396	0.207*	2.780	0.005	0.594*	9.237	0.000
PRE2	0.742			CSB3	1.310	0.507*	7.453	0.000	0.811*	19.250	0.000
PRE3	0.819			CSB4	1.373	0.160*	2.091	0.037	0.595*	9.044	0.000
PRE4	0.801			CSB5	1.137	0.070	1.246	0.213	0.257*	3.041	0.002
PC1	0.808	0.898	0.689	CSB6	1.108	0.019	0.458	0.647	0.217*	2.987	0.003
PC2	0.846			CSB7	1.063	0.104	1.645	0.100	0.214*	2.618	0.009
PC3	0.894			CSB8	1.275	0.249*	3.254	0.001	0.62*	9.484	0.000
PC4	0.768			CSB9	1.124	0.136*	2.079	0.038	0.329*	4.392	0.000

Notes: w = *weight*, l = *loading*, t = *t-value*, p = *p-value*, $^*p < 0.5$, ^{r} *excluded item*

4.2 Structural Model Assessment

The structural model should exhibit no collinearity issues, indicated with VIF values below five, which is the case for all latent variables in the model. Estimated path coefficients that take on values between −1 and +1 indicate positive and negative effects one latent construct has on another. In the proposed model, except for the paths from *Information Security Culture* and *Security Training and Awareness Programs* to *Cybersecurity Awareness*, all coefficients are significant but exhibit great differences in strength. *Information Systems Knowledge*

Table 3. Discriminant Validity - HTMT criterion

	FFI	ISC	ISK	PC	PRE	PS	PV	PSE
FFI								
ISC	0.387							
ISK	0.118	0.079						
PC	0.179	0.104	0.313					
PRE	0.342	0.326	0.338	0.246				
PS	0.191	0.214	0.05	0.067	0.271			
PV	0.054	0.064	0.123	0.163	0.099	0.175		
PSE	0.265	0.228	0.671	0.593	0.538	0.104	0.198	

has the strongest effect on *Cybersecurity Awareness*, while the other exogenous variables show low to moderate effects (see Fig. 2). The path coefficient from *Cybersecurity Awareness* to *Cybersecurity Behavior* exhibits a moderate effect. The R^2 values for *Cybersecurity Awareness* and *Cybersecurity Behavior* indicate moderate explanation of the endogenous variables through the exogenous constructs. By performing multi-group analyses (PLS-MGA [20]), differences for users of different gender or language groups can be found. While women are influenced by *Mass Media* but not by *Public Administration Information*, it is the other way around for men (men: $P_{\text{PAI}->\text{CSA}} = 0.159$, p = 0.008, $P_{\text{MMI}->\text{CSA}} = 0.003$, p = 0.467; women: $P_{\text{PAI}->\text{CSA}} = -0.005$, p = 0.44, $P_{\text{MMI}->\text{CSA}} = 0.171$, p = 0.004). When comparing the German- and French-speaking people's influences, the German-speaking are influenced by *Security Training and Awareness Programs* and *Public Administration Information*, while the French-speaking are not influenced (DE: $P_{\text{PAI}->\text{CSA}} = 0.180$, p = 0.008; FR: $P_{\text{PAI}->\text{CSA}} = 0.030$, p = 0.228; DE: $P_{\text{SETA}->\text{CSA}} = 0.142$, p = 0.041; FR: $P_{\text{SETA}->\text{CSA}} = -0.072$, p = 0.057). Moreover, the awareness of people who have experienced a cybersecurity incident in the past year (NEX) is significantly influenced by *Mass Media Influence*, whereas people with no bad experiences are not influenced (NEX: $P_{\text{MMI}->\text{CSA}} = 0.200$, p = 0.010; no NEX: $P_{\text{MMI}->\text{CSA}} = 0.016$, p = 0.445).

4.3 Mediation Analysis

In order to evaluate the role of cybersecurity awareness as a mediator between the determinants and cybersecurity behavior, a mediation analysis was performed following the guidelines proposed by [46]. The evaluation includes looking at direct and indirect effects from the exogenous variables to the endogenous variable. Table 4 shows the results of the analysis. The results suggest *Cybersecurity Awareness* is only a full or partial mediator for *Information Security Policy Provision*, *Friends and Family Influence*, *Personal Initiative* and *Information Systems Knowledge*, while other variables only have a direct (*SETA*, *MMI*) or no effect (*ISC*, *PAI*) on *Cybersecurity Behavior*.

Table 4. Mediation analysis

Path	Indirect Path Coeff.			Direct Path Coeff.			Mediation
	P	t	p	P	t	p	
ISSP -> CSB	0.063*	2.979	0.001	0.002	0.053	0.479	Full Mediation
SETA -> CSB	−0.005	0.394	0.347	0.117*	2.346	0.009	No Mediation, Direct-Only
ISC -> CSB	0.021	1.310	0.095	−0.033	0.892	0.186	No Mediation, No Effect
FFI -> CSB	0.056*	2.796	0.003	0.059	1.432	0.076	Full Mediation
MMI -> CSB	0.031	1.595	0.055	−0.074*	1.720	0.043	No Mediation, Direct-Only
PAI -> CSB	0.026	1.591	0.056	0.027	0.815	0.208	No Mediation, No Effect
PI -> CSB	0.042*	2.232	0.013	0.142*	2.892	0.002	Partial Mediation
ISK -> CSB	0.205*	6.778	0.000	0.208*	3.962	0.000	Partial Mediation

Notes: P = Path coefficient, t = t-value, p = p-value, $^{*}p < 0.5$

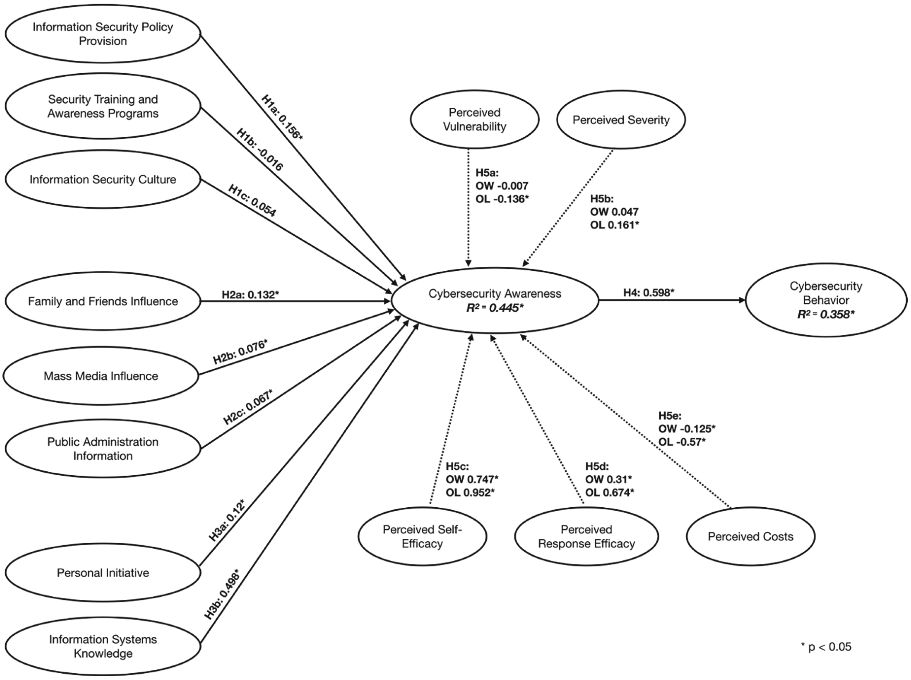
Information Security Policy Provision
Security Training and Awareness Programs
Information Security Culture
Family and Friends Influence
Mass Media Influence
Public Administration Information
Personal Initiative
Information Systems Knowledge
H1a: 0.156*
H1b: -0.016
H1c: 0.054
H2a: 0.132*
H2b: 0.076*
H2c: 0.067*
H3a: 0.12*
H3b: 0.498*
Perceived Vulnerability
Perceived Severity
H5a: OW -0.007 OL -0.136*
H5b: OW 0.047 OL 0.161*
Cybersecurity Awareness $R^2 = 0.445^*$
H4: 0.598*
Cybersecurity Behavior $R^2 = 0.358^*$
H5c: OW 0.747* OL 0.952*
H5d: OW 0.31* OL 0.674*
H5e: OW -0.125* OL -0.57*
Perceived Self-Efficacy
Perceived Response Efficacy
Perceived Costs
* p < 0.05

Fig. 2. Results - structural model evaluation

5 Discussion and Implications

The results of this study show diverse levels of impact of organizational, social and personal determinants on a user's cybersecurity awareness in his home environment. The main findings are:

- Weak influence of the workplace
- Weak to moderate social influences
- Personal initiative has a significant effect
- Strongest effect of information systems knowledge
- No significant contribution of threat appraisal to cybersecurity awareness

The limited workplace effects are in line with other studies [31,39]. It is not evident if security training and the information security culture are prevalent but not transferrable to the home environment or if they cannot be found. Mass media and public administration information exhibit disparate effects for men and women and for people who have experienced cybersecurity incidents in the past year. People from the different language groups react differently to various sources of information, emphasizing a potential cultural gap in how cybersecurity topics are handled and perceived in different cultural regions. The strong influence of information systems skills as well as the fact that the threat appraisal does not significantly contribute to cybersecurity awareness highlight the need for campaigns focusing in improving skills and understanding, confirming results of similar studies [17,39,45].

As with other studies, there are some limitations. The study relies on self-report data, which might contain a social desirability bias [10]. Additionally, the PLS-SEM method allows no goodness-of-fit measure for evaluating the fit of the model and the path estimation contains a measurement error resulting in a bias [16]. Although the sample exhibits a good balance of gender and age, works in diverse job areas, most participants work in the public sector. The influence of the workplace could be different in the private or voluntary sector.

While this study kept a generalized approach on most variables to ensure a holistic view, different types of mass media or the form of security information provided at the workplace should also be researched individually as they might lead to distinct user reactions as shown in [29,39]. Moreover, in order to create individualized and adapted campaigns, cultural differences should be investigated more closely. Considering the high potential in reaching broad masses of people, future research should investigate the reasons that inhibit a transfer of work-provided cybersecurity information to the private environment.

6 Conclusion

The human interaction with computer systems becomes increasingly important considering current trends in digitalization. This study investigates organizational, social and personal determinants of a home computer user's cybersecurity awareness and the factors impacting behavior. By providing valuable insights about cybersecurity awareness and behavior creation, the study contributes to research in the field of cybersecurity behavior and can act as a support for security practitioners while reviewing security strategies.

Appendix

Table 5. Overview survey measures

Information Security Policy Provision (ISPP) ISPP1: Information security policies are written in a manner that is clear and understandable ISPP2: Information security policies are readily available for my reference	[18]
Security Training and Awareness Programs (SETA) SETA1: My organization provides training to help employees improve their assessment and knowledge of computer and information security issues SETA2: My organization educates employees on their computer security responsibilities	[12,18]
Information Security Culture (ISC) ISC1: My colleagues and I would warn each other if we saw one of us taking risks (e.g. insecure use of email, downloading malicious software, or risky password practices) ISC2: I have a good relationship with my colleagues and other members of my organization ISC3: My organization takes the view that information security is a collective responsibility ISC4: My colleagues and I have the same ambitions and visions in terms of protecting our information assets from cyber threats (e.g. unauthorized access to information assets, becoming infected with malicious software)	[34]
Family and Friends Influence (FFI) FFI1: My family members would approve of me practicing a safe cyber behavior FFI2: My family members expect me to practice a safe cyber behavior FFI3: My friends would approve of me practicing a safe cyber behavior FFI4: My friends expect me to practice a safe cyber behavior	[29,42]
Mass Media Influence (MMI) MMI1: The mass media suggest that I should practice a safe cyber behavior MMI2: Mass media reports influence me to practice a safe cyber behavior MMI3: I feel under pressure from the mass media to practice a safe cyber behavior	[29]
Public Administration Information (PAI) PAI1: The public administration suggests that I should practice a safe cyber behavior PAI2: The public administration influences me to practice a safe cyber behavior PAI3: I feel under pressure from the public administration to practice a safe cyber behavior	[6,29]
Personal Initiative (PI) PI1: In general, I actively attack problems (of any kind) PI2: Whenever something goes wrong, I search for a solution immediately PI3: I take initiative immediately when others don't PI4: Usually I do more than I am asked to	[13]
Information Systems Knowledge (ISK) ISK1: What is your general knowledge of computers? ISK2: What is your general knowledge of the Internet (e.g. Web, email systems)?	[18]
Perceived Vulnerability (PV) PV1: I believe that I am at risk of becoming a victim of a cyber security incident (e.g. phishing, malware)	[9,17]
PV2: I believe that it is likely that I will become a victim of a cyber security incident (e.g. phishing, malware)	

(*continued*)

Table 5. (*continued*)

PV3: I believe that it is possible that I will become a victim of a cyber security incident (e.g. phishing, malware)	
Perceived Severity (PS)	[3,28]
PS1: Having my computer infected by a virus as a result of opening a suspicious email attachment is a serious problem for me	
PS2: Having my confidential information accessed by someone without my consent or knowledge is a serious problem for me	
PS3: Loss of data resulting from hacking is a serious problem for me	
Perceived Response Efficacy (PRE)	[17,39]
PRE1: I believe that protective software would be useful for detecting and removing malware	
PRE2: I believe that having passwords that are hard to guess and different for each of my accounts will help improve my security protection	
PRE3: I believe that keeping my operating systems and software updated will help improve my security protections	
PRE4: I believe that following online safety practices will help protecting me from online safety threats	
Perceived Costs (PC)	[28,45]
PC1: Practicing safe cyber behavior is inconvenient	
PC2: Practicing safe cyber behavior is time-consuming	
PC3: Practicing safe cyber behavior would require considerable investment of effort other than time	
PC4: Practicing safe cyber behavior would require starting a new habit, which is difficult	
Perceived Self-Efficacy (PSE)	[39,42]
PSE1: I feel comfortable practicing safe cyber security behavior	
PSE2: Practicing safe cyber security behavior is entirely under my control	
PSE3: I have the resources and knowledge to practice safe cyber security behavior	
PSE4: Practicing safe cyber security behavior is easy	
Cybersecurity Behavior (CSB)	[3,28]
CSB1: I use different passwords for my different online accounts (e.g., social media, online banking)	
CSB2: I usually review privacy/security settings on my online accounts (e.g., social media, online banking)	
CSB3: I keep the software and operating system on my computer up-to-date	
CSB4: I watch for unusual computer behaviors/responses (e.g., computer slowing down or freezing, pop-up windows, etc.)	
CSB5: I do not open email attachments from people whom I do not know	
CSB6: I have never sent sensitive information (such as account numbers, passwords, social security number, etc.) via email or using social media	
CSB7: I make backups of important files on my computer	
CSB8: I always respond to any malware alerts that I receive	
CSB9: I do not click on short URLs unless I know where the links will really take me	

References

1. Ajzen, I.: From intentions to actions: a theory of planned behavior. In: Kuhl, J., Beckmann, J. (eds.) Action Control. SSSSP, pp. 11–39. Springer, Heidelberg (1985). https://doi.org/10.1007/978-3-642-69746-3_2
2. Anderson, C.L., Agarwal, R.: Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. MIS Q. **34**(3), 613–643 (2010). https://doi.org/10.2307/25750694
3. Anwar, M., He, W., Ash, I., Yuan, X., Li, L., Xu, L.: Gender difference and employees' cybersecurity behaviors. Comput. Hum. Behav. **69**, 437–443 (2017). https://doi.org/10.1016/j.chb.2016.12.040

4. Baldwin, W.: Information no one else knows: the value of self-report. In: Stone, A., Bachrach, C., Jobe, J., Kurtzman, H., Cain, V. (eds.) The Science of Self-report, 1st edn, pp. 15–20. Psychology Press, Mahwah (1999)
5. Bandura, A.: Social Learning Theory. General Learning Press, New York, NY (1971)
6. Belanche Gracia, D., Casaló Ariño, L., Flavián Blanco, C.: Understanding the influence of social information sources on e-government adoption. Inf. Res. **17**(3) (2012)
7. Blythe, J.: Cyber security in the workplace: Understanding and promoting behaviour change. In: Proceedings of CHItaly 2013 Doctoral Consortium, vol. 1065, pp. 92–101 (2013)
8. Bortz, J., Döring, N.: Forschungsmethoden und Evaluation für Human-und Sozialwissenschaftler, 4th edn. Springer, Heidelberg (2006). https://doi.org/10.1007/978-3-540-33306-7
9. Crossler, R.E.: Protection motivation theory: understanding determinants to backing up personal data. In: 2010 43rd Hawaii International Conference on System Sciences (HICSS), pp. 1–10. IEEE (2010). https://doi.org/10.1109/HICSS.2010.311
10. Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M., Baskerville, R.: Future directions for behavioral information security research. Comput. Secur. **32**, 90–101 (2013). https://doi.org/10.1016/j.cose.2012.09.010, http://www.sciencedirect.com/science/article/pii/S0167404812001460
11. Da Veiga, A., Eloff, J.H.: A framework and assessment instrument for information security culture. Comput. Secur. **29**(2), 196–207 (2010). https://doi.org/10.1016/j.cose.2009.09.002
12. D'Arcy, J., Hovav, A., Galletta, D.: User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Inf. Syst. Res. **20**(1), 79–98 (2009). https://doi.org/10.1287/isre.1070.0160
13. Frese, M., Fay, D., Hilburger, T., Leng, K., Tag, A.: The concept of personal initiative: operationalization, reliability and validity in two German samples. J. Occup. Organ. Psychol. **70**(2), 139–161 (1997). https://doi.org/10.1111/j.2044-8325.1997.tb00639.x
14. Furnell, S., Bryant, P., Phippen, A.: Assessing the security perceptions of personal internet users. Comput. Secur. **26**(5), 410–417 (2007). https://doi.org/10.1016/j.cose.2007.03.001
15. Hair, J., Hollingsworth, C.L., Randolph, A.B., Chong, A.Y.L.: An updated and expanded assessment of PLS-SEM in information systems research. Ind. Manag. Data Syst. **117**(3), 442–458 (2017). https://doi.org/10.1108/IMDS-04-2016-0130
16. Hair, J.F., Hult, T., Ringle, C., Sarstedt, M.: A Primer on Partial Least Squares Structural Equation Modeling, 2nd edn. Sage, Thousand Oaks (2017)
17. Hanus, B., Wu, Y.A.: Impact of users' security awareness on desktop security behavior: a protection motivation theory perspective. Inf. Syst. Manag. **33**(1), 2–16 (2016). https://doi.org/10.1080/10580530.2015.1117842
18. Häussinger, F.J., Kranz, J.J.: Information security awareness: its antecedents and mediating effects on security compliant behavior. In: International Conference on Information Systems (ICIS) (2013)
19. Henseler, J., Ringle, C.M., Sarstedt, M.: A new criterion for assessing discriminant validity in variance-based structural equation modeling. J. Acad. Mark. Sci. **43**(1), 115–135 (2015). https://doi.org/10.1007/s11747-014-0403-8

20. Henseler, J., Ringle, C.M., Sinkovics, R.R.: The use of partial least squares path modeling in international marketing. In: Sinkovics, R.R., Ghauri, P.N. (eds.) New Challenges to International Marketing, vol. 20, pp. 277–319. Emerald Group Publishing Limited (2009). https://doi.org/10.1108/S1474-7979(2009)0000020014
21. Hertig, Y., Teufel, S.: Prosumer communities: electricity as an interpersonal construct. In: 2016 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE), pp. 89–94. IEEE (2016). https://doi.org/10.1109/ICSGCE.2016.7876032
22. Hickmann Klein, R., Mezzomo Luciano, E.: What influences information security behavior? A study with Brazilian users. JISTEM - J. Inf. Syst. Technol. Manag. **13**(3), 479–496 (2016). https://doi.org/10.4301/s1807-17752016000300007
23. Howe, A.E., Ray, I., Roberts, M., Urbanska, M., Byrne, Z.: The psychology of security for the home computer user. In: 2012 IEEE Symposium on Security and Privacy (SP), pp. 209–223. IEEE (2012). https://doi.org/10.1109/SP.2012.23
24. Kajtazi, M., Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Assessing sunk cost effect on employees' intentions to violate information security policies in organizations. In: 2014 47th Hawaii International Conference on System Sciences (HICSS), pp. 3169–3177. IEEE (2014). https://doi.org/10.1109/HICSS.2014.393
25. Ki-Aries, D., Faily, S.: Persona-centred information security awareness. Comput. Secur. **70**, 663–674 (2017). https://doi.org/10.1016/j.cose.2017.08.001
26. Leiner, D.J.: Sosci survey (version 3.1.01-i) [computer software] (2018). http://www.soscisurvey.com
27. Muhirwe, J., White, N.: Cybersecurity awareness and practice of next generation corporate technology users. Issues Inf. Syst. **17**(2), 183–192 (2016)
28. Ng, B.Y., Kankanhalli, A., Xu, Y.C.: Studying users' computer security behavior: a health belief perspective. Decis. Support. Syst. **46**(4), 815–825 (2009). https://doi.org/10.1016/j.dss.2008.11.010
29. Ng, B.Y., Rahim, M.: A socio-behavioral study of home computer users' intention to practice security. In: PACIS 2005 Proceedings, pp. 234–247 (2005)
30. Organisation for Economic Co-operation and Development: OECD guidelines for the security of information systems and networks: Towards a culture of security (2002). http://www.oecd.org/sti/ieconomy/15582260.pdf
31. Rader, E., Wash, R.: Identifying patterns in informal sources of security information. J. Cybersecur. **1**(1), 121–144 (2015). https://doi.org/10.1093/cybsec/tyv008
32. Ringle, C.M., Wende, S., Becker, J.M.: Smartpls 3 (version 3.2.5) [computer software] (2015). http://www.smartpls.com
33. Rocha Flores, W., Antonsen, E., Ekstedt, M.: Information security knowledge sharing in organizations: investigating the effect of behavioral information security governance and national culture. Comput. Secur. **43**, 90–110 (2014). https://doi.org/10.1016/j.cose.2014.03.004
34. Rocha Flores, W., Ekstedt, M.: Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. Comput. Secur. **59**, 26–44 (2016). https://doi.org/10.1016/j.cose.2016.01.004
35. Rogers, R.W.: A protection motivation theory of fear appeals and attitude change1. J. Psychol.: Interdiscip. Appl. **91**(1), 93–114 (1975). https://doi.org/10.1080/00223980.1975.9915803
36. Rogers, R.W.: Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. In: Cacioppo, J.T., Petty, R. (eds.) Social Psychophysiology: A Sourcebook, chap. 6, pp. 153–177. Guilford, New York (1983)

37. Schlienger, T., Teufel, S.: Information security culture. In: Ghonaimy, M.A., El-Hadidi, M.T., Aslan, H.K. (eds.) Security in the Information Society. IAICT, vol. 86, pp. 191–201. Springer, Boston, MA (2002). https://doi.org/10.1007/978-0-387-35586-3_15
38. Sherif, E., Furnell, S., Clarke, N.: Awareness, behaviour and culture: the ABC in cultivating security compliance. In: The 10th International Conference for Internet Technology and Secured Transactions (ICITST-2015), pp. 90–94. IEEE (2015). https://doi.org/10.1109/ICITST.2015.7412064
39. Shillair, R., Dutton, W.H.: Supporting a cybersecurity mindset: getting internet users into the cat and mouse game. SSRN Electron. J. (2016). https://doi.org/10.2139/ssrn.2756736
40. Simonet, J.: The Influence of Organizational, Social and Personal Factors on Cybersecurity Awareness and Behavior of Home Computer Users. Master's thesis, iimt, University of Fribourg (2018)
41. Talib, S., Clarke, N.L., Furnell, S.M.: An analysis of information security awareness within home and work environments. In: ARES 2010 International Conference on Availability, Reliability, and Security, pp. 196–203. IEEE (2010). https://doi.org/10.1109/ARES.2010.27
42. Taylor, S., Todd, P.A.: Understanding information technology usage: a test of competing models. Inf. Syst. Res. **6**(2), 144–176 (1995). https://doi.org/10.1287/isre.6.2.144
43. Teufel, S., Teufel, B.: Crowd energy information security culture - security guidelines for smart environments. In: 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity), pp. 123–128 (2015). https://doi.org/10.1109/SmartCity.2015.58
44. Weinstein, N.D.: Testing four competing theories of health-protective behavior. Health Psychol. **12**(4), 324–333 (1993). https://doi.org/10.1037//0278-6133.12.4.324
45. Woon, I., Tan, G., Low, R.: A protection motivation theory approach to home wireless security. In: Proceedings of the Twenty-Sixth International Conference on Information Systems (ICIS), pp. 367–380 (2005)
46. Zhao, X., Lynch, J., Chen, Q.: Reconsidering Baron and Kenny: myths and truths about mediation analysis. J. Consum. Res. **37**(2), 197–206 (2010). https://doi.org/10.1086/651257