Social Network Self-Protection Model: What Motivates Users to Self-Protect?

Damjan Fujs[1], Anže Mihelič[1,2] and Simon Vrhovec[1]

[1]*University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia*
[2]*University of Ljubljana, Faculty of Law, Ljubljana, Slovenia*
E-mail: simon.vrhovec@um.si

Received 14 January 2019; Accepted 31 May 2019;
Publication 20 June 2019

Abstract

Social networks are an indispensable activity for billions of users making them an attractive target for cyberattacks. There is however only scarce research on self-protection of individuals outside the organizational context. This study aims to address this gap by explaining what motivates individuals to self-protect on social networks. A survey (N = 274) has been conducted among Slovenian Facebook users to test the proposed social network self-protection model. The results show that privacy concerns and perceived threats significantly affect user's intention to self-protect. Descriptive norm only affects intention indirectly through perceived threats appearing to contradict a large body of research on behavioral intentions. "If others protect themselves, there must be a serious threat." On the other hand, it also helps to explain why the direct effect of descriptive norm on security-related behavior is relatively small in other studies. Surveillance concerns, regulation and information sensitivity all significantly affect privacy concerns. Although privacy concerns are currently high due to the recent high-profile privacy-related scandals (e.g., Cambridge Analytica, Facebook, Google+), it may not affect the motivation of users to self-protect as they dealt with issues far beyond their control.

Journal of Cyber Security and Mobility, Vol. 8_4, 467–492.
doi: 10.13052/jcsm2245-1439.844

Nevertheless, users with higher levels of privacy concerns than their peers may be more motivated to self-protect.[1]

Keywords: Self-protective behavior, social networks, privacy concerns, surveillance concerns, information sensitivity, regulation, perceived threats, vulnerability, severity.

1 Introduction

People are massively engaged in online activities, especially on social networks [2–4]. The largest social network (namely, Facebook) alone has 1.45 billion active daily users and 2.20 billion monthly active users [5]. The pervasiveness of the social networks makes them an attractive target for cyberattacks of various kinds (e.g., hacking into social networks accounts, online harassment, loss of privacy, etc. [6–9]) potentially affecting billions of users [10]. Sometimes social network users do not have the adequate knowledge to protect their social network accounts and themselves from cyberthreats even though security mechanisms are available [11]. Additionally, social network users may simply lack the needed motivation to seek knowledge on how to protect themselves or to engage in self-protective behavior in the cyberspace [12–14]. It appears that many users plainly disregard security recommendations [15]. For example, many social network users still use simple passwords and the same password on multiple websites [16]. Even though social network users may be concerned about their own privacy, their engagement in self-protective behavior still seems to be lacking. Paradoxically, it seems that social network users have little sense of privacy despite their privacy concerns [17].

Research on self-protection in the cyberspace primarily addresses the users in organizational contexts as an important part of ensuring information security in organizations [13, 18, 19]. Even the research focusing on the individual level, is done from the socio-organizational perspectives in the context of organizations [20, 21]. Therefore, there is a gap in the motivational theories that would focus on individuals outside of the organizational context. Such insights would also benefit the research on the motivation of individuals in organizational contexts as people tend to behave similarly at work and at home [22].

[1] This publication is an extended version of [1].

This paper focuses on the effect of privacy concerns and perceived threats of individual social network users on intention for engaging in self-protective behavior. In this paper, we also explore the factors affecting both privacy concerns (i.e., information sensitivity, state regulation, surveillance concerns) and perceived threats (i.e., perceived vulnerability, perceived severity, descriptive norm) to offer a deeper insight into the motivation of social network users to self-protect.

2 Theoretical Background

2.1 Perceived Threats

We used the protection motivation theory (PMT) as a framework to study user's motivation to self-protect on social networks. PMT aims to explain how fear appeals change someone's protection-related behaviors through perceived vulnerability and severity, measure efficacy and self-efficacy [23]. In this paper, we focus on threat appraisal which often includes perceived vulnerability, severity and threats in research on motivation to engage in self-protective behavior in various research areas [13, 24, 25]. *Perceived vulnerability* indicates the odds that someone will become a victim of an unwanted event (i.e., the likelihood of a cybersecurity incident) [18, 20, 21, 26–28]. It may impact security behavior in both personal and organizational contexts [29–31]. *Perceived severity* is the extent of the consequences for someone in the case of an unwanted event (i.e., the effects of a cybersecurity incident) [13, 18, 20, 21, 27, 28]. *Perceived threats* are closely related to both perceived vulnerability and severity and has been commonly presented as the key trigger for the internal motivation for self-protective behavior [13, 24, 25].

2.2 Privacy Concerns

The ever-increasing amount of data that social network users store and share on various social networks is creating numerous opportunities for cybercriminals and other threat actors in the cyberspace. Privacy protection is therefore becoming increasingly important [32]. When considering the well-known social networks, such as Facebook, Twitter or Instagram, it may be easy to trust them to have solid and effective security mechanisms in place. Users are primarily motivated to disclose information to social networks because of the convenience of maintaining and developing relationships, and platform enjoyment [33]. These benefits of data sharing are however countervailed by privacy concerns of social network users. *Privacy concerns* are an individual's awareness and assessment of risks related to privacy violations [34]. Social network users have differing attitudes towards their privacy on social networks which may affect their intention to engage in self-protective behavior [35, 36]. For example, individuals can be grouped according to their levels of privacy concerns into three groups [37]. *Privacy fundamentalists* are very privacy conscious and highly value their privacy [37]. *Privacy pragmatists* view privacy as very important but will surrender some of it when they can benefit from it however only as far as they believe that the given information will not be misused [37]. *Privacy unconcerned* do not care much about privacy and do not treat it as important [37].

Privacy concerns may be related to several factors, such as regulation, information sensitivity and surveillance concerns [35, 38]. *Information sensitivity* describes how delicate certain private information (e.g., private messages, private photos) is to someone [39]. *State regulation* designates how well the legislation protects someone's privacy [38]. *Surveillance concerns* refer to how concerned is someone about the state surveillance over him in the cyberspace [39].

3 Research Model and Hypotheses Development

Building on the theoretical background, we propose a research model based on various disciplines, such as psychology [28], sociology [40], and political science [35]. The proposed research model is presented on Figure 1. In the next paragraphs, we present the developed research hypotheses underlying the proposed research model. The hypotheses are based on their theoretical meaning and relevant literature.

Individuals first need to detect and evaluate cybersecurity threats in order to engage in self-protective behaviors [13]. If the threat assessment results in a high degree of vulnerability and/or a high degree of severity, an individual will be more motivated to self-protect and vice versa [41]. Therefore, we assume that both the perceived likelihood of a cybersecurity incident and the perceived severity of its consequences contribute to the users' perceived threats.

The acts of social network users in a certain situation may depend on the collective behavior and collective consciousness [42]. Descriptive norm refers to the beliefs of an individual about how widespread a particular behavior (e.g., self-protecting) is among his peers [42]. It may affect the intention to self-protect [43]. However, we assume that there is an indirect effect of the descriptive norm through perceived threat. For example, if an individual

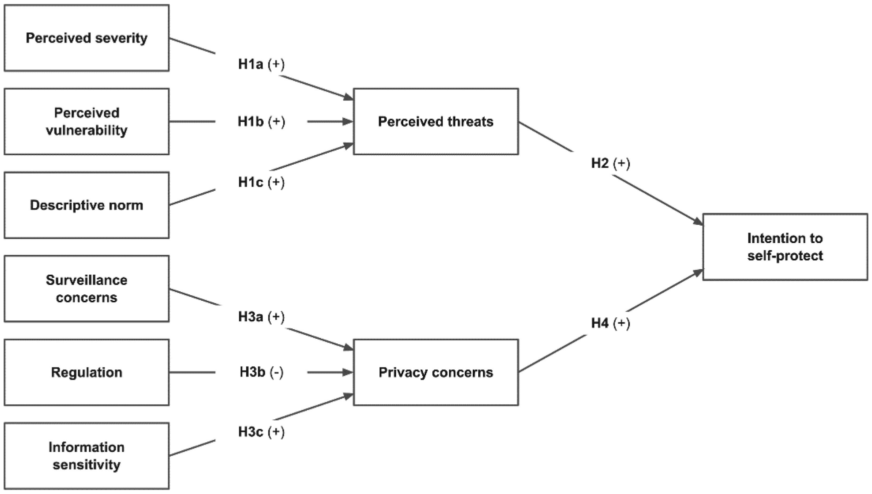


Figure 1 Social network self-protection model.

perceives that others are protecting themselves well, he will perceive the threat to be higher. We therefore hypothesize:

H1a: Higher perceived severity is associated with higher perceived threat.
H1b: Higher perceived vulnerability is associated with higher perceived threat.
H1c: Stronger descriptive norm is associated with higher perceived threat.

Perceived threats may affect the decision of social network users to engage in self-protective behavior. Even if social network users believe that some malicious activities (e.g., the distribution of a computer virus, hacking of a social network account) do not pose an immediate threat to them, the sole existence of the threat may affect their decision to engage in self-protective behavior. Social network users must therefore recognize the threats otherwise they will not act to avoid them (Liang and Xue, 2010). Since behavioral intention is a strong predictor of actual behavior [44], we propose the following hypothesis:

H2: Higher perceived threats are associated with higher intention to self-protect.

Even though privacy concerns can vary from one individual to another [37], they may be a powerful inhibitor for cyberspace activity. Similarly to individuals who may be uncertain about providing their personal medical data online due to its sensitivity and the potential threat to their privacy that its misuse poses [45], social network users may be more concerned about their privacy if they perceive that their personal and/or private data stored (or shared) on social networks is more sensitive. Privacy concerns may be also related to the trust that social network users put into the state regulation [46, 47]. For example, social network users that trust the regulation (i.e., the national and international legal regulation) to protect the privacy of their data stored on social networks are probably less concerned about the privacy of their data on them.

If social network users however perceive that the state is in fact doing quite the opposite of protecting the privacy of their data, i.e., invading their privacy through surveillance, their privacy concerns may increase [48]. This led us to the following hypotheses:

H3a: Higher surveillance concerns are associated with higher privacy concerns.
H3b: Better perceived state regulation is associated with lower privacy concerns.
H3c: Higher information sensitivity is associated with higher privacy concerns.

Privacy concerns may directly affect the intention of users to engage in self-protective behavior on social networks. Users that are more concerned about their privacy will likely put more effort into their self-protection. We therefore propose the final hypothesis:

H4: Higher privacy concerns are associated with higher intention to self-protect.

4 Method

The overall approach to test the research model was a field study using survey methodology for data collection. In this section, we first present the details of instrument development and then the data collection procedure.

4.1 Instrument Development

To reduce issues with reliability and validity of the questionnaire, the measures used in this study were taken from previously validated research and adapted to the context of our research. Intention to self-protect (*Int*) was considered the main dependent variable in this study. Its items were adapted from [21]. The surveillance concerns (*SurvCon*) construct captures the social network users' concerns about the government's monitoring of the internet and was adapted from [39]. Items for regulation (*Reg*) were adapted from [38]. These items capture social network users' perceptions of national and international regulation of social networks. The information sensitivity (*InfSen*) construct was used to capture social network users' perceptions of the sensitivity of their information on the social networks (e.g., private chats, searches). Its items were adapted from [39]. To capture the degree of social networks users' concerns about their privacy on social networks, the privacy concerns (*PriCon*) items adapted from [36] were used. To understand the social network users' perceived risk of someone hacking into their social network accounts, three constructs were used in our study. Perceived severity (*Sev*) and perceived threats (*Thrt*) were adapted from [24] while perceived vulnerability (*Vul*) was adapted from [49]. In order to understand the role of social influence on the social network users' perceived threat, descriptive norm (*DesNorm*) was used. Descriptive norm questions were adapted from [50]. All items were measured using a five-point Likert scale from 1 (*I strongly disagree*) to 5 (*I strongly agree*). Control variables which included the demographic characteristics (i.e., gender, age, education, employment status) were added to control for an explanation of the results due to extraneous factors.

The questionnaire is available in English and Slovenian. The questionnaire was first developed in English and then translated into Slovenian by three translators independently. The translators developed the Slovenian questionnaire through consensus. The Slovenian questionnaire has been pre-tested by 5 independent respondents who provided feedback on its clarity. Based on the received feedback, the Slovenian questionnaire was reviewed to remove any ambiguity. Items were reworded, added and deleted in the pre-test. To ensure the consistency between the Slovenian and English questionnaire, the Slovenian questionnaire was back-translated. No significant differences in the meaning between the original items in English and back-translations were noticed. The English questionnaire was however reviewed to update the items and to remove any ambiguity based on the back-translation. Both versions of the questionnaire are presented in the Appendix.

An online survey was prepared once consensus was reached regarding validity and clarity of the instrument. To achieve a common understanding of each term among respondents, the terms were explicitly defined where necessary (e.g., social networks, security measures, government monitoring).

4.2 Data Collection Procedure

The research model was tested using an online survey. We conducted the survey among members of 15 Facebook groups with various topics (e.g., waste-free home, employment searching, undergraduate and postgraduate study, distinctive Slovenian dialect, student dorm, free alcohol, political parties, software developers) between June and November 2018. A total of 308 respondents completed the survey. After excluding poorly completed responses, we were left with 274 useful responses providing for a response rate of 12.1 percent (2,271 clicks on the survey). The average age of the respondents was 26.56 years, ranging from 18 to 69 years. Other demographic characteristics of the respondents are presented in Table 1.

Due to the sensitive nature of the survey topic, safeguards were put in place to encourage participation and hones responses. First, the survey was hosted

Table 1 Demographics

Characteristic	Count	%
Gender		
Male	79	28.8
Female	157	57.3
Not specified	38	13.9
Status		
Student	155	56.6
Employed	59	21.5
Unemployed	19	6.9
Retired	4	1.5
Not specified	37	13.5
Education		
Less than bachelor’s degree	104	38.0
Bachelor’s degree	99	36.1
Master’s degree	29	10.6
PhD	4	1.5
Not specified	38	13.9

on an online platform that does not store the IP addresses of the respondents. Next, the respondents were informed about the voluntariness and anonymity of participating in the survey. Finally, the respondents were assured that the collected data will be used for research purposes only. No special incentives were offered to encourage participation in the survey.

4.3 Data Analysis

IBM SPSS Statistics Version 25 was used for data analysis. The psychometric properties of the measures were evaluated before testing the research model. All constructs were modelled as reflective. To assess them, we examined their convergent validity, discriminant validity and reliability.

To explore the factor structure, principal axis factoring (PAF) with an oblique rotation (Direct Oblimin) was conducted. PAF does not assume normally distributed variables. Since the constructs were assumed to be correlated, an oblique rotation was deemed adequate as it assumes factors are correlated. The factorability was assessed with Kaiser-Meyer-Olkin Index (KMO) and Bartlett's test of sphericity. The number of factors was determined according to the theoretical research model.

Convergent validity evaluates consistency across multiple items. To ensure it, only items with factor loading near and above 0.4 were considered for inclusion in each factor. Discriminant validity is the extent to which different constructs diverge from one another. It is shown when items load higher on the hypothesized factor than on any other factor. Additionally, an inter-construct correlation above 0.70 may suggest that a pair of constructs may represent a single construct. Construct reliability evaluates to which degree the items yield consistent results. To analyze it, Cronbach's alpha (CA) scores were calculated for the items included in each construct. CA scores near and above 0.60 indicate satisfactory reliability while values above 0.70 are recommended.

Our hypotheses were tested using multiple linear regression (multiple independent variables and a single dependent variable). Assumptions of multiple linear regression (e.g., linearity, normality, homoscedasticity, multicollinearity) were carefully considered.

5 Results

5.1 Instrument Validation

The Kaiser-Meyer-Olkin Index (KMO = 0.794) and Bartlett's test of sphericity was significant (approximate chi square = 3,045.43, $p < 0.001$) verified the sampling adequacy of the analysis. PAF with an oblique rotation was conducted to extract 9 theoretically assumed factors. Table 2 shows the factor loadings of measurement items.

Due to its low factor loading, Thrt3 was excluded from further data analysis. Loadings of all other items on their assigned factors were higher than any other loading suggesting good convergent and discriminant validity.

Table 2 Factor loadings (PFA extraction with Direct Oblimin rotation)

Item	1	2	3	4	5	6	7	8	9
Sev1	–	–	–	–	–	−**.599**	–	–	–
Sev2	–	–	–	–	–	−**.607**	–	–	–
Sev3	–	–	–	–	–	−**.863**	–	–	–
Vul1	–	–	**.527**	–	–	–	–	–	–
Vul2	–	–	**.651**	–	–	–	–	–	–
Vul3	–	–	**.824**	–	–	–	–	–	–
DesNorm1	–	–	–	–	–	–	−**.768**	–	–
DesNorm2	–	–	–	–	–	–	−**.781**	–	–
DesNorm3	–	–	–	–	–	–	−**.770**	–	–
Thrt1	**.775**	–	–	–	–	–	–	–	–
Thrt2	**.788**	–	–	–	–	–	–	–	–
Thrt3	–	–	–	–	–	−.340	–	–	–
SurvCon1	–	–	–	–	–	–	–	**.906**	–
SurvCon2	–	–	–	–	–	–	–	**.953**	–
SurvCon3	–	–	–	–	–	–	–	**.850**	–
Reg1	–	**.762**	–	–	–	–	–	–	–
Reg2	–	**.889**	–	–	–	–	–	–	–
Reg3	–	**.775**	–	–	–	–	–	–	–
InfSen1	–	–	–	–	**.580**	–	–	–	–
InfSen2	–	–	–	–	**.870**	–	–	–	–
InfSen3	–	–	–	–	**.751**	–	–	–	–
PriCon1	–	–	–	–	–	–	–	–	**.599**
PriCon2	–	–	–	–	–	–	–	–	**.698**
PriCon3	–	–	–	–	–	–	–	–	**.391**
Int1	–	–	–	**.842**	–	–	–	–	–
Int2	–	–	–	**.882**	–	–	–	–	–
Int3	–	–	–	**.874**	–	–	–	–	–

Note: Factor loadings below an absolute value of 0.30 are omitted.

Table 3 Inter-construct correlations with CA in the diagonal

Construct	1	2	3	4	5	6	7	8	9
1: Sev	**.73**	–	–	–	–	–	–	–	–
2: Vul	−.256	**.74**	–	–	–	–	–	–	–
3: DesNorm	.121	.125	**.82**	–	–	–	–	–	–
4: Thrt	−.405	.210	−.230	**.80**	–	–	–	–	–
5: SurvCon	−.103	−.043	−.232	.338	**.93**	–	–	–	–
6: Reg	−.009	−.060	−.346	−.102	−.111	**.85**	–	–	–
7: InfSen	−.300	.240	−.056	.388	.269	−.049	**.78**	–	–
8: PriCon	−.096	.092	−.050	.361	.298	−.196	.396	**.68**	–
9: Int	−.067	−.023	−.114	.228	.141	−.181	.170	.389	**.91**

Also, all inter-construct correlations presented in Table 3 are well-below the threshold of 0.70 which further suggests good discriminant validity.

All CA values were near or above the recommended threshold of 0.70 suggesting adequate reliability therefore the reliability of all constructs was considered acceptable.

The factor loading of PriCon3 was rather low suggesting potential issues with convergent validity therefore the possibility of excluding an item from PriCon was considered. The analysis showed improvement in convergent validity of PriCon after excluding PriCon3 however its reliability dropped. Since convergent validity, discriminant validity and reliability of PriCon with all items were at least marginally acceptable, we retained all PriCon items in further analyses.

5.2 Testing of Research Model

The research model was tested with three multiple linear regression models. All linear regression models were significant ($p < 0.001$). The results of hypothesis testing are presented in Figure 2.

The results show that approximately 23 percent of the variance of privacy concerns is explained by surveillance concerns, regulation and information sensitivity. Therefore, we can confirm hypotheses H1a ($p < 0.001$), H1b ($p < 0.001$) and H1c ($p < 0.01$).

Next, around 19 percent of the variance of perceived threats is explained by perceived severity, perceived vulnerability and descriptive norm supporting hypotheses H3a ($p < 0.001$), H3b ($p < 0.01$) and H3c ($p < 0.001$).

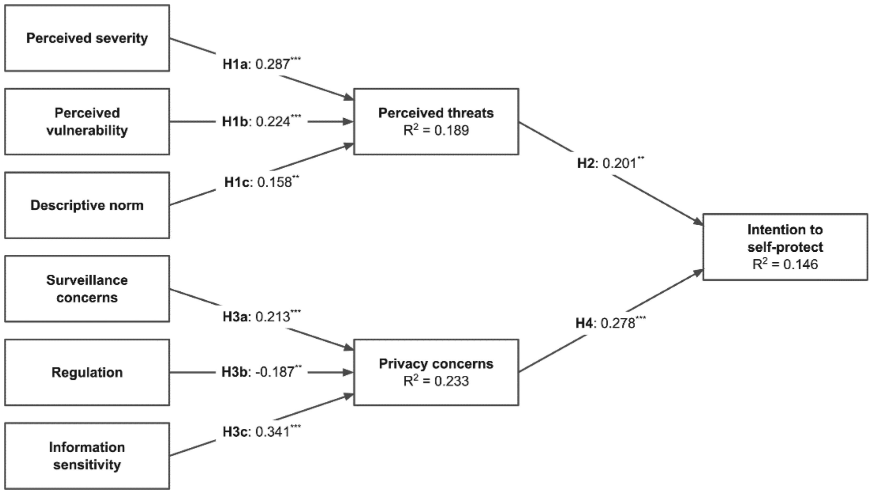


Figure 2 Hypothesis testing results (standardized beta coefficient β, adjusted R^2); ** $p < 0.01$; *** $p < 0.001$.

Finally, around 15 percent of the variance of intention to self-protect is explained by perceived privacy concerns and perceived threats supporting hypotheses H2 ($p < 0.01$) and H4 ($p < 0.001$), respectively.

6 Discussion

6.1 Theoretical Implications

This study provides three key theoretical contributions. First, we build on two different well-established research areas to form a new theory incorporating both threat appraisal from PMT and privacy concerns, and their impact on the motivation of social network users to self-protect (i.e., to implement recommended security measures). Existing research already confirmed the effects of perceived threats (e.g., [13, 24, 25]) and privacy concerns (e.g., [35, 45, 47]) on various security-related behaviors. Our results however suggest that both perceived threats and privacy concerns impact the security-related behaviors of social network users. Therefore, both aspects should be considered when studying them. This contributes to the understanding of social network users' motivation to self-protect.

Second, our findings reveal that descriptive norm (i.e., how other social network users implement recommended security measures) affects the intention to self-protect indirectly through perceived threats. There is a large body of research (e.g., [20, 26, 50]) that associates descriptive norm directly to behavioral intentions. Compared to other factors, its effect is however rather small in the context of security-related behaviors. In our study, descriptive norm is closely associated with perceived threats despite an absence of a direct effect on the intention to self-protect. This on one hand appears to confirm our assumption that social network users evaluate threats also by looking at what others do. "If others protect themselves, then there must be a serious threat" – and vice versa. On the other hand, it also helps to explain why the direct effect of descriptive norm on security-related behavior is relatively small in other studies. This enriches the understanding of both threat appraisal and the role of descriptive norm in the self-protection motivation.

Third, this study improves our understanding of factors influencing privacy concerns of social network users. Unlike prior studies that focused predominantly on the effect of privacy concerns on behavior (e.g., [34, 35, 45, 47, 51]) or on single factors affecting privacy concerns, such as information sensitivity (e.g., [45]) and regulation (e.g., [35, 47]), we explore the effects of surveillance concerns, regulation and information sensitivity on privacy concerns. All these factors significantly affect privacy concerns. This enriches the understanding of privacy concerns by incorporating different antecedents.

6.2 Practical Implications

This study provides several practical implications for social network providers, governments and non-governmental organizations (NGOs). First, social network providers should note that privacy concerns of social network users have at least a comparable effect on their self-protection as perceived threats. In the wake of several high-profile privacy-related scandals in the last year (e.g., Cambridge Analytica [52], Google+ API bugs [53, 54], Facebook and Google buying financial data of their users [55, 56]), it seems that the privacy concerns of social network users are relatively high [57]. This however does not mean that this general rise in privacy concerns automatically motivates users to self-protect. These scandals were not related to users' actions. Rather, they dealt with issues far beyond the control of social network users. To deal with such wide-spread fluctuations, privacy concerns of a social network user may be compared relatively to his broader social network group. It would be also possible to detect social network users that are less likely to self-protect automatically on a broad scale by profiling them according to their privacy concerns. For example, each social network user's level of privacy concerns may be deducted by examining his recent behavior on a social network (e.g., frequency of public/private posts, tagging, commenting on others' posts). This would enable social network providers to improve the security of their high-risk users, e.g., by trying to raise their privacy awareness indirectly raising also their privacy concerns and motivating them to self-protect. However, this may have undesired effects as research shows that privacy concerns are directly related to the intention to disclose (i.e., share) information [35, 45] which is the essence of social networks. A simple solution would be to simply pay more attention to the activity of high-risk social network users and play only a reactive role. This may not be the only solution though. Disclosure of information is related to different threat actors (i.e., the social network providers themselves) than the threat actors that social network users need to self-protect from (e.g., cybercriminals). Social network providers may therefore aim to raise the privacy concerns of their users while simultaneously build the trust between them which is another important factor affecting the intention to disclose information [35, 45]. This would enable social network providers to motivate their users to self-protect against alien threats while building their mutual trust which would arguably not affect social network users' disclosing of information. However, further research would still be needed to gain a deeper insight into this.

Second, governments may also note the effects of privacy concerns on the motivation of social network users to self-protect. Governments may have however differing goals regarding this. A key goal in promoting the digital market is to build a trustworthy digital market environment. Social networks have become an important integrational part of such digital market environments. In this regard, the government is in a similar position to the social network providers. They may seek to raise the privacy concerns of social network users to motivate them to self-protect against malicious actors while simultaneously build trust between social network users and businesses active on social networks. Further promoting existing privacy awareness campaigns and starting new ones may help achieve this effect. However, governments also need to tackle the challenges posed by various threat actors operating on social networks, such as criminals, cybercriminals, extremists and terrorists. Even though social network providers may cooperate with governments to tackle these threats, it may not be in their interest that all social network users self-protect themselves as it may obstruct their investigations (e.g., using end-to-end encryption). Nevertheless, it is less likely that threat actors would protect themselves due to a higher level of privacy concerns as they have other much stronger motivators to do so, such as not to get caught.

Third, our results show that surveillance concerns affect privacy concerns of social network users. Governments may therefore raise social network users' privacy concerns by raising their surveillance concerns, e.g., through public disclosure of use of algorithms for surveillance [58] or their activity in high-profile cases. Such an effect was achieved recently in the United Kingdom through the Skripal case. The public was shown the pervasiveness of video surveillance in the United Kingdom that enabled the persecutors to identify and monitor the movements of the suspects from entering to leaving the country. Raising surveillance concerns may also have a deterring effect on threat actors operating on social networks similarly such effects in the real world (e.g., the impact of CCTV on crime [59]). However, contrary to the likely complementarity of raising privacy awareness and simultaneously building mutual trust, raising surveillance concerns may also lower the trust between governments and social network users. This would be an unwanted effect that could however suppress the benefits of such an approach. Especially as the democratic governments tend to appease the public.

Fourth, NGOs interested in improving the self-protective behavior of social network users may have a more unbiased role in raising privacy concerns. If social network providers and governments need to consider pros and cons of raising privacy concerns, NGOs do not need to do so. NGOs may simply raise social network users' concerns by privacy awareness campaigns, campaigns to raise the government surveillance awareness etc. The role played by NGOs may be further complemented by social network providers' and governments' campaigns to build mutual trust in their fight against the common enemy – the various threat actors in the cyberspace.

6.3 Limitations and Future Research

This study has some limitations that the reader should note and may be explored further. The data were collected in Slovenia which may affect the generalizability of this study. Future studies may therefore select research samples from different demographic groups to appraise the cultural differences of social network users elsewhere in the world. Additionally, conducting an international survey of social network users may provide additional insights into the impact of different legislations and political systems on the engagement of self-protective behavior. The survey has been distributed only through Slovenian Facebook groups. Research including other social networks and on a global scale would thus be highly beneficial. The self-reported intentions to self-protect do not necessarily translate into actual behavior [60]. Further works may conduct an experimental study to provide better understanding of the self-protective behavior of social network users.

7 Conclusion

This study adds valuable empirical findings to the current literature on intentions of users to self-protect on social networks. The present work gives social network providers and other stakeholders a set of practical courses of action to address issues related to self-protection of social network users. It also suggests new theoretical ways in which researchers and students can explore the domain of studying the motivation of social network users to self-protect on social networks. Using the groundwork laid down in our research, future studies could further extend out theoretical understanding of and the practical ability to improve the users' intention to self-protect on social networks.

Appendix

Table A1. The English questionnaire's items

Construct	Item	
Surveillance concerns (*Adapted from* [39])	SurvCon 1	I am very concerned about government monitoring of my public and private activity on social networks.
	SurvCon 2	I am very concerned about government monitoring of my activity on search engines.
	SurvCon 3	I am very concerned about government monitoring of my emails.
Regulation (*Adapted from* [38])	Reg 1	Our legislation is adequately protecting the privacy of social network users.
	Reg 2	The international legislation is adequately protecting the private information of social network users.
	Reg 3	The government does enough to protect social network users from privacy violations.

Table A1. (*Continued*)

Construct	Item	
Information sensitivity (*Adapted from* [39])	InfSen 1	I consider the content of my private chats as very sensitive.
	InfSen 2	I consider information on which profiles I visit as very sensitive.
	InfSen 3	I consider information on which posts I pay more attention to as very sensitive.
Privacy concerns (*Adapted from* [36])	PriCon 1	It highly bothers me when social networks ask me about my personal data.
	PriCon 2	I always think twice before submitting my personal data to social networks.
	PriCon 3	I am very concerned that social networks collect too much personal data about me.
Perceived severity (*Adapted from* [24])	Sev 1	An intrusion would highly jeopardize my privacy.
	Sev 2	My personal data collected via an intrusion could be misused for criminal purposes.
	Sev 3	My personal data collected via an intrusion could be misused against me.
Perceived vulnerability (*Self-developed*)	Vul 1	My accounts are very vulnerable to intrusions.
	Vul 2	I am certain that I can become a victim of an intrusion.
	Vul 3	The data on my accounts is constantly threatened.
Descriptive norm (*Adapted from* [50])	DesNorm 1	I believe that people implement recommended security measures.
	DesNorm 2	It is very likely that the majority of social network users is trying to protect themselves from hackers.
	DesNorm 3	I am convinced that people protect their social network accounts with recommended security measures.
Perceived threats (*Adapted from* [24])	Thrt 1	I feel threatened by intrusions.
	Thrt 2	Intrusions threaten my accounts.
Intention to self-protect (*Adapted from* [21])	Int 1	I intend to implement recommended security measures regularly.
	Int 2	I predict that I will implement recommended security measures in the near future.
	Int 3	I plan to implement recommended security measures.

Table A2. The Slovenian questionnaire's items

Construct	Item	
Surveillance concerns	SurvCon 1	Zelo me skrbi, da država nadzoruje mojo javno in zasebno aktivnost na socialnih omrežjih.
	SurvCon 2	Zelo me skrbi, da država nadzoruje mojo aktivnost na spletnih iskalnikih.
	SurvCon 3	Zelo me skrbi, da država nadzoruje mojo elektronsko pošto.
Regulation	Reg 1	Naša zakonodaja zadostno ščiti zasebnost uporabnikov socialnih omrežij.
	Reg 2	Mednarodna zakonodaja zadostno ščiti zasebne informacije uporabnikov socialnih omrežij.
	Reg 3	Država stori dovolj, da bi zaščitila uporabnike socialnih omrežij pred kršitvami zasebnosti.
Information sensitivity	InfSen 1	Vsebino svojih zasebnih klepetov dojemam kot zelo občutljivo.
	InfSen 2	Informacije o tem, čigave profile obiskujem, dojemam kot zelo obèutljive.
	InfSen 3	Informacije o tem, katerim objavam posvetim več pozornosti, dojemam kot zelo občutljive.
Privacy concerns	PriCon 1	Zelo me moti, ko me socialna omrežja sprašujejo po osebnih podatkih.
	PriCon 2	Preden posredujem svoje osebne podatke socialnim omrežjem, vedno premislim dvakrat.
	PriCon 3	Zelo me skrbi, da socialna omrežja o meni zbirajo preveč osebnih podatkov.
Perceived severity	Sev 1	Vdor bi močno ogrozil mojo zasebnost.
	Sev 2	Moji osebni podatki, pridobljeni z vdorom, bi bili lahko zlorabljeni v kriminalne namene.
	Sev 3	Moji osebni podatki, pridobljeni z vdorom, bi lahko bili zlorabljeni zoper mene.
Perceived vulnerability	Vul 1	Moji računi so zelo ranljivi za vdore.
	Vul 2	Prepričan sem, da lahko postanem žrtev vdora.
	Vul 3	Podatki na mojem računu so stalno ogroženi.
Descriptive norm	DesNorm 1	Verjamem, da ljudje na socialnih omrežjih uporabljajo priporočene varnostne mehanizme.
	DesNorm 2	Zelo verjetno se večina uporabnikov socialnih omrežij skuša zaščititi pred hekerji.
	DesNorm 3	Prepričan sem, da ljudje ščitijo svoje račune na socialnih omrežjih s priporočenimi varnostnimi mehanizmi.

Table A2. (Continued)

Construct	Item	
Perceived threats	Thrt 1	Zaradi vdorov se počutim ogroženega.
	Thrt 2	Vdori ogrožajo moje račune.
Intention to self-protect	Int 1	Redno nameravam uporabljati priporočene varnostne mehanizme.
	Int 2	Predvidevam, da bom v bližnji prihodnosti uporabljal priporočene varnostne mehanizme.
	Int 3	Načrtujem uporabo priporočenih varnostnih mehanizmov.

References

[1] Fujs, D., Vrhovec, S., and Mihelič, A. (2018). What drives the motivation to self-protect on social networks? The role of privacy concerns and perceived threats. In Proceedings of the Central European Cybersecurity Conference 2018 – CECC 2018 (p. a11). New York, NY, USA: ACM. https://doi.org/10.1145/3277570.3277581

[2] M. Shahriari, S. Haefele, and R. Klamma, "Using Content to Identify Overlapping Communities in Question Answer Forums," *J. Univers. Comput. Sci.*, vol. 23, no. 9, pp. 907–931, 2017.

[3] A. Krouska, C. Troussas, and M. Virvou, "Comparative evaluation of algorithms for sentiment analysis over social networking services," *J. Univers. Comput. Sci.*, vol. 23, no. 8, pp. 755–768, 2017.

[4] R. Rupnik, "Oblačna integracijska platforma kot koncept integracije za aplikacije in sisteme v kmetijstvu," *Elektroteh. Vestn. /Electrotech. Rev.*, vol. 85, no. 4, pp. 212–216, 2018.

[5] Facebook, "Company Info," *Facebook Newsroom*, 2018. [Online]. Available: https://newsroom.fb.com/company-info/.

[6] I. Bernik and G. Mesko, "Internet study of familiarity with cyber threats and fear of cybercrime," *Rev. za kriminalistiko kriminologijo*, vol. 62, no. 3, pp. 242–252, 2011.

[7] S. Vrhovec, "Safe mobile device use in the cyberspace/Varna uporaba mobilnih naprav v kibernetskem prostoru," *Elektroteh. Vestn./Electrotech. Rev.*, vol. 83, no. 3, pp. 144–147, 2016.

[8] T. Tomažič and N. B. Vilela, "Ongoing Criminal Activities in Cyberspace: From the Protection of Minors to the Deep Web," *Rev. za Kriminalistiko Kriminologijo*, vol. 68, no. 4, pp. 412–423, 2017.

[9] B. Japelj, “Crime in Slovenia in 2017,” *Rev. za kriminalistiko kriminologijo*, vol. 69, no. 2, pp. 67–99, 2018.

[10] S. Thielman, “Yahoo hack: 1bn accounts compromised by biggest data breach in history,” *The Guardian*, New York, 2016.

[11] P. Wisniewski, H. Xu, M. B. Rosson, and J. M. Carroll, “Parents Just Don’t Understand: Why Teens Don’t Talk to Parents about Their Online Risk Experiences,” in *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing – CSCW ’17*, 2017, pp. 523–540.

[12] A. Mihelič and S. Vrhovec, “A model of self-protection in the cyberspace/Model samozaščite v kibernetskem prostoru,” *Elektroteh. Vestn./Electrotech. Rev.*, vol. 85, no. 1–2, pp. 13–22, 2018.

[13] A. Mihelič and S. Vrhovec, “Explaining the employment of information security measures by individuals in organizations: The self-protection model,” in *Advances in Cybersecurity 2017*, I. Bernik, B. Markelj, and S. Vrhovec, Eds. Maribor, Slovenia: University of Maribor Press, 2017, pp. 23–34.

[14] G. Burger, M. Pogačnik, and J. Guna, “Študija orodij za sledenje pogleda na primeru študije meritve uporabniške izkušnje mobilne aplikacije 1,2,3 Ljubljana,” *Elektroteh. Vestn./Electrotech. Rev.*, vol. 84, no. 4, pp. 173–180, 2017.

[15] C. Zhang, J. Sun, X. Zhu, and Y. Fang, “Privacy and Security for Online Social Networks: Challenges and Opportunities,” *IEEE Netw.*, vol. 24, no. 4, pp. 13–18, 2010.

[16] L. van Zoonen, “Privacy concerns in smart cities,” *Gov. Inf. Q.*, vol. 33, no. 3, pp. 472–480, Jul. 2016.

[17] S. Livingstone, “Taking risky opportunities in youthful content creation: teenagers’ use of social networking sites for intimacy, privacy and self-expression,” *New Media Soc.*, vol. 10, no. 3, pp. 393–411, Jun. 2008.

[18] S. R. Boss, D. F. Galletta, P. B. Lowry, G. D. Moody, and P. Polak, “What Do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors,” *MIS Q.*, vol. 39, no. 4, pp. 837–864, 2015.

[19] G. D. Moody, M. Siponen, and S. Pahnila, “Toward a Unified Model of Information Security Policy Compliance,” *MIS Q.*, vol. 42, no. 1, pp. 285–311, 2018.

[20] T. Herath and H. R. Rao, “Protection motivation and deterrence: a framework for security policy compliance in organisations,” *Eur. J. Inf. Syst.*, vol. 18, no. 2, pp. 106–125, Apr. 2009.

[21] A. C. Johnston and M. Warkentin, "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Q.*, vol. 34, no. 3, pp. 549–566, 2010.

[22] S. L. R. Vrhovec, "Challenges of mobile device use in healthcare," in *39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO 2016)*, 2016.

[23] J. E. Maddux and R. W. Rogers, "Protection motivation theory and self-efficacy: A revised theory of fear appeals and attitude change," *J. Exp. Soc. Psychol.*, vol. 19, no. 5, pp. 469–479, 1983.

[24] H. Liang and Y. Xue, "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *J. Assoc. Inf. Syst.*, vol. 11, no. 7, pp. 394–413, 2010.

[25] Y. Chen and F. M. Zahedi, "Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China," *MIS Q.*, vol. 40, no. 1, pp. 205–222, 2016.

[26] N. Thompson, T. J. McGill, and X. Wang, "Security begins at home': Determinants of home computer and mobile device security behavior," *Comput. Secur.*, vol. 70, pp. 376–391, Sep. 2017.

[27] D. Lee, R. Larose, and N. Rifon, "Keeping our network safe: a model of online protection behaviour," *Behav. Inf. Technol.*, vol. 27, no. 5, pp. 445–454, 2008.

[28] S. K. Wurtele and J. E. Maddux, "Relative Contributions of Protection in Motivation Theory Components Predicting Exercise Intentions Behavior," *Heal. Psychol.*, vol. 6, no. 5, pp. 453–466, 1987.

[29] M. Workman, W. H. Bommer, and D. Straub, "Security lapses and the omission of information security measures: A threat control model and empirical test," *Comput. Human Behav.*, vol. 24, no. 6, pp. 2799–2816, 2008.

[30] M. Anwar, W. He, I. Ash, X. Yuan, L. Li, and L. Xu, "Gender difference and employees' cybersecurity behaviors," *Comput. Human Behav.*, vol. 69, pp. 437–443, Apr. 2017.

[31] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *MIS Q.*, vol. 34, no. 3, pp. 523–548, 2018.

[32] C. K. Georgiadis, N. Polatidis, H. Mouratidis, and E. Pimenidis, "A Method for Privacy-preserving Collaborative Filtering Recommendations," *J. Univers. Comput. Sci.*, vol. 23, no. 2, pp. 146–166, 2017.

[33] H. Krasnova, S. Spiekermann, K. Koroleva, and T. Hildebrand, "Online Social Networks: Why We Disclose," *J. Inf. Technol.*, vol. 25, no. 2, pp. 109–125, Jun. 2010.

[34] X. Tan, L. Qin, Y. Kim, and J. Hsu, "Impact of privacy concern in social networking web sites," *Internet Res.*, vol. 22, no. 2, pp. 211–233, 2012.

[35] H. J. Smith, T. Dinev, and H. Xu, "Information Privacy Research: An Interdisciplinary Review," *MIS Q.*, vol. 35, no. 4, pp. 989–1015, 2011.

[36] W. Hong and J. Y. L. Thong, "Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies," *MIS Q.*, vol. 37, no. 1, pp. 275–298, 2013.

[37] T. Buchanan, C. Paine, A. N. Joinson, and U.-D. Reips, "Development of measures of online privacy concern and protection for use on the Internet," *J. Am. Soc. Inf. Sci. Technol.*, vol. 58, no. 2, pp. 157–165, Jan. 2007.

[38] M. Lwin, J. Wirtz, and J. D. Williams, "Consumer online privacy concerns and responses: A power–responsibility equilibrium perspective," *J. Acad. Mark. Sci.*, vol. 35, no. 4, pp. 572–585, 2007.

[39] T. Nam, "Untangling the relationship between surveillance concerns and acceptability," *Int. J. Inf. Manage.*, vol. 38, no. 1, pp. 262–269, 2018.

[40] J. Fogel and E. Nehmad, "Internet social network communities: Risk taking, trust, and privacy concerns," *Comput. Human Behav.*, vol. 25, no. 1, pp. 153–160, 2009.

[41] T. Sommestad, H. Karlzén, and J. Hallberg, "The sufficiency of the theory of planned behavior for explaining information security policy compliance," *Inf. Comput. Secur.*, vol. 23, no. 2, pp. 200–217, 2015.

[42] R. N. Rimal and K. Real, "Understanding the Influence of Perceived Norms on Behaviors," *Commun. Theory*, vol. 13, no. 2, pp. 184–203, May 2003.

[43] P. Sheeran and S. Orbell, "Augmenting the Theory of Planned Behavior: Roles for Anticipated Regret and Descriptive Norms," *J. Appl. Soc. Psychol.*, vol. 29, no. 10, pp. 2107–2142, Oct. 1999.

[44] I. Ajzen, "The theory of planned behavior," *Organ. Behav. Hum. Decis. Process.*, vol. 50, no. 2, pp. 179–211, Dec. 1991.

[45] G. Bansal, F. M. Zahedi, and D. Gefen, "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online," *Decis. Support Syst.*, vol. 49, no. 2, pp. 138–150, May 2010.

[46] A. J. Rohm and G. R. Milne, "Just what the doctor ordered – The role of information sensitivity and trust in reducing medical information privacy concern," *J. Bus. Res.*, vol. 57, no. 9, pp. 1000–1011, Sep. 2004.

[47] J. Wirtz, M. O. Lwin, and J. D. Williams, "Causes and consequences of consumer online privacy concern," *Int. J. Serv. Ind. Manag.*, vol. 18, no. 3–4, pp. 326–348, Aug. 2007.

[48] T. Dinev, P. Hart, and M. R. Mullen, "Internet privacy concerns and beliefs about government surveillance – An empirical investigation," *J. Strateg. Inf. Syst.*, vol. 17, no. 3, pp. 214–233, Sep. 2008.

[49] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Comput. Secur.*, vol. 31, no. 1, pp. 83–95, 2012.

[50] C. L. Anderson and R. Agarwal, "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Q.*, vol. 34, no. 3, pp. 613–643, 2010.

[51] C. Dwyer, S. R. Hiltz, and K. Passerini, "Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace," in *AMCIS 2007 Proceedings*, 2007, p. Paper 339.

[52] J. T. Tarigan and E. M. Zamzami, "Post Cambridge Analytica fallout: Observing Facebook users awareness regarding data security," *Int. J. Eng. Technol.*, vol. 7, no. 3.32, pp. 123–126, 2018.

[53] D. MacMillan and R. McMillan, "Google Exposed User Data, Feared Repercussions of Disclosing to Public," *The Wall Street Journal*, 2018. [Online]. Available: https://www.wsj.com/articles/google-exposed-user-data-feared-repercussions-of-disclosing-to-public-1539017194. [Accessed: 08-Jan-2018].

[54] T. Romm and C. Timberg, "Google reveals new security bug affecting more than 52 million users," *The Washington Post*, 2018. [Online]. Available: https://www.washingtonpost.com/technology/2018/12/10/google-reveals-new-security-bug-affecting-more-than-million-users/. [Accessed: 08-Jan-2018].

[55] M. Bergen and J. Surane, "Google and Mastercard Cut a Secret Ad Deal to Track Retail Sales," *Bloomberg Technology*, 2018. [Online]. Available: https://www.bloomberg.com/news/articles/2018-08-30/google-and-mastercard-cut-a-secret-ad-deal-to-track-retail-sales. [Accessed: 08-Jan-2019].

[56] E. Glazer, D. Seetharaman, and A. Andriotis, "Facebook to Banks: Give Us Your Data, We'll Give You Our Users," *The Wall Street Journal*, 2018.

[Online]. Available: https://www.wsj.com/articles/facebook-to-banks-give-us-your-data-well-give-you-our-users-1533564049. [Accessed: 08-Jan-2018].

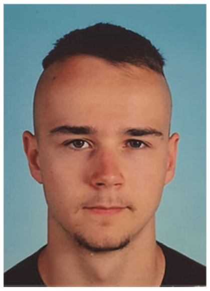
[57] A. Perrin, "Americans are changing their relationship with Facebook," *Pew Research Center*, 2018. [Online]. Available: http://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook/. [Accessed: 08-Jan-2018].

[58] A. Završnik, "Algoritmično nadzorstvo: veliko podatkovje, algoritmi in družbeni nadzor," *Rev. za kriminalistiko kriminologijo*, vol. 68, no. 2, pp. 135–149, 2017.

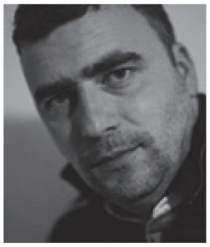
[59] B. C. Welsh and D. P. Farrington, "Public Area CCTV and Crime Prevention: An Updated Systematic Review and Meta-Analysis," *Justice Q.*, vol. 26, no. 4, pp. 716–745, Dec. 2009.

[60] A. Kojič, T. Hovelja, and D. Vavpotič, "Ogrodje za izboljšanje procesov razvoja informacijskih sistemov z uporabo hevristik za izboljšave splošnih poslovnih procesov," *Elektroteh. Vestn./Electrotech. Rev.*, vol. 83, no. 1–2, pp. 47–53, 2016.

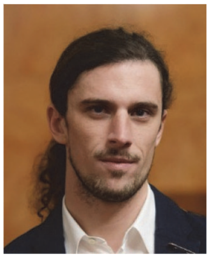
Biographies



Damjan Fujs received his B.Sc. degree in Information Security in 2017 from the Faculty of Criminal Justice and Security at the University of Maribor and is currently M.A. student in Criminal Justice and Security at the University of Maribor, Slovenia. The primary focus on his research has been in the areas of protection motivation on social networks and secure technology usage with a specific concentration on the behavioral aspects of online privacy and cybersecurity.



Anže Mihelič is a PhD student at both the Faculty of Law and at the Faculty of Computer and Information Science at the University of Ljubljana. He is Assistant at the Faculty of Criminal Justice and Security at the University of Maribor. His primary interests include privacy law, secure software development, and social aspects of cybersecurity.



Simon Vrhovec is Assistant Professor at the University of Maribor. He received his PhD in Computer and Information Science from the University of Ljubljana in 2015. He has co-chaired the Central European Cybersecurity Conference (CECC) in 2018 and 2019. His research interests include human factors in cybersecurity, agile methods and secure software development, resistance to change, and medical informatics.