© Fehér-Polgár, P. (2021): Measuring Safetyconsciousness. In Kelemen-Erdos, A., Feher-Polgar, P., & Popovics A. (eds.): FIKUSZ 2021 Proceedings (pdf) ISBN 978-963-449-274-0, Obuda University, Keleti Károly Faculty of Business and Management, 252 p. pp. 22-27., 6 p. http://kgk.uni-obuda.hu/fikusz

Measuring Safetyconsciousness

Pál Fehér-Polgár

Óbuda University, Keleti Károly Faculty of Business and Management,
feherpolgar.pal@kgk.uni-obuda.hu

Abstract: In the last three decades the penetration, possibilities and importance of ICT technologies have spread with a rapid growth. ICT have claimed a major part of our private and professional lives. With the growth of possibilities and the dependence on the ICT technologies the problem of information security and the security of information technology have also risen. Security consciousness of the user plays a major role in the security of systems. In a previous research I have modified the widely used DOSPERT questionnaire for a comparable measurement of the IT security risk awareness with other risk types. In present article, information security-related questions from the modified DOSPERT questionnaire, along with other questions designed to measure security awareness, to compare the results have been used.

Keywords: BYOD, Safety Consciousness, DOSPERT

1 Measuring safetyconsciousness

One of the main risks is security threats from the user. To use a simple analogy, a chain is only as strong as its weakest link, and various studies have shown that one of the most prominent sources of risk in IT systems is the user and his or her security awareness (Michelberger, Kemendi 2020)(Ali, Szikora 2017).

Security awareness in different domains of life can be measured using a variety of tools. Among these, the DOSPERT questionnaire developed by Weber, Blais and Betz in 2002 (Blais 2002, Weber 2002) has been used for a previous research. This is a self-report questionnaire that measures the likelihood of following certain behaviors, their expected benefits and the perceived magnitude of the risk of these behaviors. In a previous research I have modified this questionnaire to be able to measure risks in the ICT domain in a previous research (Fehér-Polgár 2020).

© Fehér-Polgár, P. (2021): Measuring Safetyconsciousness. In Kelemen-Erdos, A., Feher-Polgar, P., & Popovics A. (eds.): FIKUSZ 2021 Proceedings (pdf) ISBN 978-963-449-274-0, Obuda University, Keleti Károly Faculty of Business and Management, 252 p. pp. 22-27., 6 p. http://kgk.uni-obuda.hu/fikusz

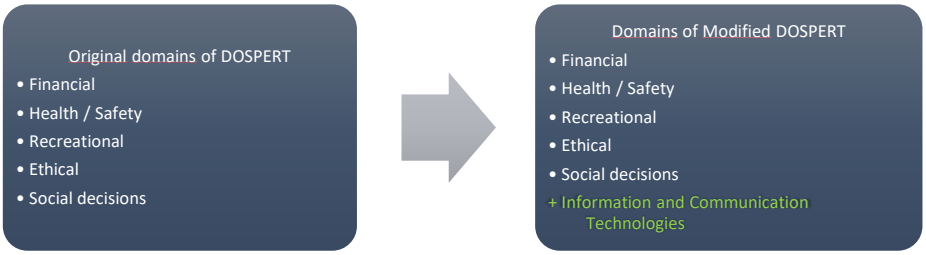

Figure 1
Domains of the original and the modified DOSPERT questionnaire
(Fehér-Polgár 2020)

For this purpose, I have created 5 new questions on behavioral patterns that are highly threatening to security, yet common and can be committed by almost any user at any firm:

- Would you send corporate data to your private email
- Would you connecting to public open Wi-Fi
- Would you let somebody to use your mobile without your previous consent
- Would you use your pin (password) - unlock pattern in front of others
- Would you copy corporate data to private smartphones

2 Current research on safetyconsciousness

Present research reflects the results of a comparative analysis initiated on the basis of a Buzánszky 2021 (Buzánszky 2021).

The sample of questionnaire respondents was selected using snowball method. The age of respondents had a scale from 18 to 60 years, the mean age was 33,58 years and the standard deviation was 10.33 years. Males had been over represented in the sample, as they were the 61% of the respondents. 66% of the respondents had answered that they have never studied IT security before in an organized way. The overall results are limited due to the sample size.

© Fehér-Polgár, P. (2021): Measuring Safetyconsciousness. In Kelemen-Erdos, A., Feher-Polgar, P., & Popovics A. (eds.): FIKUSZ 2021 Proceedings (pdf) ISBN 978-963-449-274-0, Obuda University, Keleti Károly Faculty of Business and Management, 252 p. pp. 22-27., 6 p. http://kgk.uni-obuda.hu/fikusz

3 Methodology and findings

For the comparison, taking into account the specificity of the sample and the questions, Spearman's correlation was used. Ten questions were derived from the modified DOSPERT questionnaire, 5 were about the likelihood of adopting different behaviors and 5 on the perceived risks of these behaviors. These were compared with the questions on safety-conscious behavioral patterns constructed by Buzánszky (2021).

When examining the correlation between these, weak and moderate correlations have been found in several areas, the most interesting and significant of which were the following.

Table 1. Correlation between feeling risky for connecting open WiFi networks and the usage of two-factor authentication (n=129)

			Feeling risky for connecting open WiFi networks
Spearman's rho	Usage of two-factor authentication	Correlation Coefficient	,233**
		Sig. (2-tailed)	,008

**. Correlation is significant at the 0.01 level (2-tailed).

Source: own research, 2021

The correlation between feeling high risk of connecting to open WiFi networks and the usage of two-factor authentication has been found significant.

This can be translated as those who are feeling risky to connect open WiFi networks have a risen safety consciousness and more likely to apply two factor authentications where that is applicable.

© Fehér-Polgár, P. (2021): Measuring Safetyconsciousness. In Kelemen-Erdos, A., Feher-Polgar, P., & Popovics A. (eds.): FIKUSZ 2021 Proceedings (pdf) ISBN 978-963-449-274-0, Obuda University, Keleti Károly Faculty of Business and Management, 252 p. pp. 22-27., 6 p. http://kgk.uni-obuda.hu/fikusz

Table 2. Correlation between connecting to open WiFi networks and installing security updates for the operating system (n=129)

			Connecting to open WiFi networks
Spearman's rho	Installing security updates for the operating system.	Correlation Coefficient	-,205*
		Sig. (2-tailed)	,035

*. Correlation is significant at the 0.05 level (2-tailed).

Source: own research, 2021

In between the probability of connecting to an open WiFi network and installing of security updates for the operating system has had an indirect correlation.

This means that those who are likely to install security updates for their softwares are less likely to connect to open, and therefore likely unsecure WiFi networks.

Table 3. Correlation between copying corporate data to private smartphone and installing security updates for the operating system (n=129)

			Copying corporate data to private smartphone
Spearman's rho	Installing security updates for the operating system.	Correlation Coefficient	,197*
		Sig. (2-tailed)	,021

*. Correlation is significant at the 0.05 level (2-tailed).

Source: own research, 2021

Correlation had been found in the sample in-between of installing security updates and coping corporate data to private smartphone owned by the user.

While with the previous pair of questions we could see positive, security conscious behavior, here we can see the opposite. Sending corporate data to one's private smartphone is a high risk behavior, as the corporate data is sent out from the computer system of the firm and this way is out of the control of the corporation.

© Fehér-Polgár, P. (2021): Measuring Safetyconsciousness. In Kelemen-Erdos, A., Feher-Polgar, P., & Popovics A. (eds.): FIKUSZ 2021 Proceedings (pdf) ISBN 978-963-449-274-0, Obuda University, Keleti Károly Faculty of Business and Management, 252 p. pp. 22-27., 6 p. http://kgk.uni-obuda.hu/fikusz

Table 4. Correlation between copying corporate data to private smartphone and the usage of password management software (n=129)

			Copying corporate data to private smartphone
Spearman's rho	Usage of password management software.	Correlation Coefficient	-,200*
		Sig. (2-tailed)	,020

*. Correlation is significant at the 0.05 level (2-tailed).

Source: own research, 2021

In between of copying corporate data to the user's own smartphone and the usage of password management software there could be seen a week, but significant inverse correlation.

This can be translated as those who are less likely to copy corporate data out from the firm's computer network are more likely to use password management softwares.

These answers can be considered as a positive behavior for the safety consciousness.

Table 5. Correlation between sending corporate data to private email and how safety conscious of dealing with an incoming email with an attachment (n=129)

			Sending corporate data to private email
Spearman's rho	How safety conscious of dealing with an incoming email with an attachment	Correlation Coefficient	-,231**
		Sig. (2-tailed)	,009

**. Correlation is significant at the 0.01 level (2-tailed).

Source: own research, 2021

Correlation between of another pair of interesting and safety conscious behavior can be seen. Those who are more likely process less risky their email attachments are less likely for sending out corporate data from the computer network of the firm too. Dealing with precautions with email attachment is must. According to IT specialists and researchers of the field of safety and security sciences are considering all email attachments as risks for the ICT security. Completely relying on virus and malware scanners are not enough. The safetyconscious behavior and lowering the risks cause of this is a must.

© Fehér-Polgár, P. (2021): Measuring Safetyconsciousness. In Kelemen-Erdos, A., Feher-Polgar, P., & Popovics A. (eds.): FIKUSZ 2021 Proceedings (pdf) ISBN 978-963-449-274-0, Obuda University, Keleti Károly Faculty of Business and Management, 252 p. pp. 22-27., 6 p. http://kgk.uni-obuda.hu/fikusz

Conclusions

The research made with the help of Péter Buzánszky have had produced a low numbered sample, which means we cannot extrapolate the outcomes of this sample for the whole population, and the findings can only be used with limitations.

Although we could see two basic groups in the sample. One with a higher and one with a lower level of ICT safetyconsciousness. Those who have a higher level can be considered as a lower risk for the firm as they less likely to act risky while working for the firm.

While the other group, with a lower safetyconscious level can be seen a risk source, which needs to be taken care. This could be done, among with other precautions, with the help of further ICT security studies.

For the first step for lowering this risk firms need to find those employees and future employees who can be a source of ICT risk with their higher potential risky behaviors. The modified DOSPERT questionnaire - after further research and refinement - could be used to find current and future employees with a higher potential risk.

References

[1] Ali, B. & Szikora, P. (2017) Információbiztonság az Y generáció körében In: Csiszárik-Kocsir, Ágnes (ed.) Vállalkozásfejlesztés a XXI. században: VII. tanulmánykötet Óbudai Egyetem (2017) pp. 24-40. , 17 p.

[2] Blais; Weber (2006) A Domain-Specific Risk-Taking (DOSPERT) scale for adult populations. Judgment and Decision Making, 1, 33-47.

[3] Buzánszky, P. (2021) Kibertámadások a XXI. században

[4] Fehér-Polgár, P. (2020) Examination of IT risk-taking with modified DOSPERT questionnaire among university students In: Keszthelyi, András; Szikora, Péter; Fehér-Polgár, Pál (eds.) 18th International Conference on Management, Enterprise, Benchmarking. Proceedings (MEB 2020) Budapest, Óbudai Egyetem 231 p. pp. 48-56. , 9 p.

[5] Lazányi K, Virglerová Z, Dvorský J, Dapkus R (2017) An analysis of factors related to “taking risks”, according to selected sociodemographic factors ACTA POLYTECHNICA HUNGARICA 14 : 7 pp. 35-50. , 16 p.

[6] Michelberger, P., & Kemendi, A. (2020). Data, information and it security - software support for security activities. Problems of Management in the 21st Century, 15(2), 108-124. https://doi.org/10.33225/pmc/20.15.108

[7] Renn (1992) „Concept of Risk: A Classification,” in Social Theories of Risk, G. Krimsky, Szerk., Westport, Praeger, 1992, pp. 53-82.

[8] Weber, E. U., Blais, A.-R., & Betz, N. (2002). A domain-specific risk attitude scale: Measuring risk perceptions and risk behaviors. Journal of Behavioral Decision Making, 15, 263-290.