Towards Personalized User Training for Secure Use of Information Systems

Damjan Fujs
Faculty of Computer and Information Science, University of Ljubljana, Slovenia
damjan.fujs@fri.uni-lj.si

Simon Vrhovec
Faculty of Criminal Justice and Security, University of Maribor, Slovenia
simon.vrhovec@um.si

Damjan Vavpotič
Faculty of Computer and Information Science, University of Ljubljana, Slovenia
damjan.vavpotic@fri.uni-lj.si

Abstract: *Information Systems (IS) represent an integral part of our lives, both in the organizational and personal sphere. To use them securely, users must be properly trained. The main problem is that most training processes still use the one-size-fits-all approach where users receive the same kind of learning material. In addition, personalized training may be a more suitable approach however a comprehensive process for IS user profiling and personalized IS user training improvement has not been introduced yet. This paper proposes a novel approach for personalized user training for secure use of IS to fill in this gap. The proposed approach focuses on three key dimensions (i.e., the personalization process, selection of training tools and materials, and participants) and is composed of five phases covering the identification of key IS security elements, IS user profiling and personalization of IS security training. It is scalable to all company sizes and aims to lower both the IS training costs and optimization of outcomes. As a side-effect, it also helps to lower user resistance to participation in IS security training.*

Keywords: *Education, training, awareness, adaptation, tailoring, information security, cost-benefit.*

Received July 27, 2020; accepted October 10, 2021
https://doi.org/10.34028/iajit/19/3/3

1. Introduction

The modern world is intertwined with computer-based Information Systems (IS), resulting in both a growing number of integrated devices and a growing number of IS users. Consequently, the attack surface of current IS and the number of cybersecurity incidents [30] leading to financial losses are also increasing [13] thus it is important to be able to address these cyber threats to IS [21]. Although there are several technical measures for ensuring information security available, such specialized mechanisms may not be enough [11]. It is therefore important that IS users are trained to use it securely [3].

Training and education for secure use of IS generally have the goal of providing various techniques to tackle or avoid cyber and Information Security (IS security) threats [1]. Several training approaches, such as serious games, themed awareness videos and virtual labs, exist [1]. Nevertheless, the vast majority of training approaches follow a one-size-fits-all strategy that considers all participants uniformly (e.g., all participants receive the same learning materials) [23]. Such approaches appear to be unsuitable as users tend to fail to use their training outcomes in practice [6]. IS users have varying levels of IS security knowledge, awareness and motivation depending on several factors, such as previous training, experience, personal traits, etc., It is therefore an especially challenging task to train all IS users in companies as a single mistake, such as a wrong click on an emailed link, by any company employee can in turn lead to a cybersecurity incident. Recent research suggests that IS security training could leverage IS user personalization (e.g., by considering IS user role, prior knowledge, barriers, learning style, IS security perception) to tackle these issues [23, 24]. Additionally, training for secure use of IS may be more effective with the personalization of training materials and the training approach itself [17].

Existing personalized training approaches however do not provide a comprehensive process for adapting IS security training to the context nor an in-depth methodology for IS user profiling or personalized training improvement. In addition, there is a lack of conceptual models that strive for pedagogical effectiveness [16]. In this paper, we propose a novel approach for personalized training for secure use of IS aiming to address these challenges. The proposed approach is theoretically based on three key dimensions (i.e., the personalization process, selection of training tools and materials, and participants). Five phases covering the identification of key IS security elements, IS user profiling and personalization of IS security training form the foundation of a comprehensive IS security training personalization strategy.

2. Related Work

In this section, we discuss the prior work related to personalized user training for secure use of IS. We focus on the following two aspects: personalization of training materials and personalization of the training approach. Various terms, such as personalized, tailored, adapted and customized, are used interchangeably in existing research.

2.1. Personalization of Training Materials

In computer science, training materials can be described as learning tools for supporting effective training (e.g., textbooks, slides, video, tutorials, quizzes) [14, 19]. It however remains unclear how to most effectively carry out material-based training to achieve the best possible learning outcomes. Although there are several examples of cybersecurity training [28], personalization enabling the customization of training materials seems to be a perspective approach. Personalization in information systems research was initially focused on customer relationships in order to improve the user experience [10]. Personalization approaches for enriching the learning process with the help of information systems later emerged which enabled the development of skills process through e-learning [20]. The emergence of smart tools in learning environments [2] offered the prospect of a better concept of personalization. Mobile-game based learning [22] may be also beneficial especially considering the wide availability of mobile devices. It is only in the recent years that approaches started emerging for personalized training for secure use of information systems [1, 14].

Approaches adopting the broader educational personification principles to improve IS security based on IS user characteristics (e.g., role, prior knowledge, barriers, learning style, IS security perception) can be found in the literature [23]. Nevertheless, it remains unclear how to implement these approaches in practice. In addition, these approaches were first extended with peer learning (i.e., less experienced IS users learn from their more experienced peers) and security champions (knowledgeable individuals motivated to transfer their knowledge) [24]. A key drawback is the lack of ability to ensure quality and effectiveness of personalized training.

2.2. Personalization of the Training Approach

Personalization of the training approach is a different paradigm from personalization of training materials since it focuses on the way in which training itself is delivered. The traditional teaching approach envisages the same kind of training for all participants. There are some newer training approaches that deliver relevant and high-quality personalized content through various media, such as cybersecurity education through live competitions (e.g., Hackathons, Blue Team/Red Team) and serious games. In live competitions and serious games, participants demonstrate knowledge and skills in real time and on practical examples. These approaches are however among the most organizationally and cost-intensive ones as all steps and pedagogical benefits must be carefully planned to provide the needed infrastructure, resources, evaluation criteria, etc., [16]. Other personalized training approaches include slow education (expert mentoring), online tutoring, virtual laboratories, learning by doing, videogames, etc., [7]. Video games have several levels of difficulty. For example, games that are distinctly mental (e.g., games where the player has to solve a puzzle to go to the next level), or shooting games with add-on IS security puzzles [4]. A key disadvantage of these approaches is that it is hard to clearly define training objectives and thus to determine their main contribution.

In addition to their outcome effectiveness, it is also important that training approaches are cost effective. Various algorithms [8, 17], intelligent tutoring systems [27], e-learning systems [25] and models of data analytics [5, 20] have been proposed to minimize the cost and complexity of training while considering training personalization. This enables the determination of the most adequate training approaches according to the organization and user needs in order to sustainably train IS users. Existing approaches however do not address the question whether a certain training investment will pay off or not (net outcome). Although cost effective training is a priority, it still needs to be focused to reach the needed outcomes.

3. Method

To formulate the proposed approach, inductive reasoning was employed to analyze the data from a variety of relevant scientific and professional literature reviewed. First, we determined the search keywords (e.g., information security and information systems) to reach relevant research on personalization of training in cybersecurity, information security and information systems in general. Next, we searched for the identified keywords in scientific databases web of science, Scopus, Google Scholar and IEEE Xplore. Journal and conference papers were collected according to their relevance of the studied topic. The literature review procedure was complemented by searching for gray literature found in the references of relevant papers. Finally, we formulated the proposed approach with a comparative analysis of the data retrieved from the gathered papers.

4. Formulation of the Proposed Approach for Personalized Training for Secure Use of Information Systems

To better present the topics covered by the training for secure use of IS, the term IS security element is used. An IS security element is any measure that increases the security of an IS if used adequately (e.g., secure password, firewall, spam protection). Suitable training for all IS security elements is therefore needed for a reasonably secure use of an IS. In this section, we first present the three key dimensions that the proposed IS security training approach is based on. Next, we present the five phases of the proposed approach.

4.1. Theoretical Foundations of Personalized Information Systems Security Training

The proposed approach focuses on three key dimensions as presented in Figure 1. The personalization process, selection of training tools and materials, and participants. The personalization process focuses on two key personalization options. As it is possible to adapt both the training approach [7, 16, 24] and the IS security elements themselves. For example, the IS security element secure password can be addressed in two ways if users are not using secure passwords. Either the training is personalized to the participating IS users, their reasons for not using secure passwords (e.g., lack of knowledge, lack of motivation) and their relative attractiveness as a target (e.g., higher management IS users with broad IS access may need more personalized training to ensure they have adequate knowledge and motivation to use strong passwords while IS users with very restricted IS access may need only simpler and more cost-effective basic training), or the IS security element is first adapted itself (e.g., by requiring the users to use strong passwords) and then the training (if needed) tailored to fit it. The key goal of the selection of training tools and materials is to identify which training tools and materials are most compatible with individual participants or participant groups. For example, some IS users may prefer lectures in person, online live lectures, or learning by themselves without the help of a trainer. Participants are IS users who need IS security training due to several reasons, such as unawareness, lack of motivation, lack of knowledge, etc.

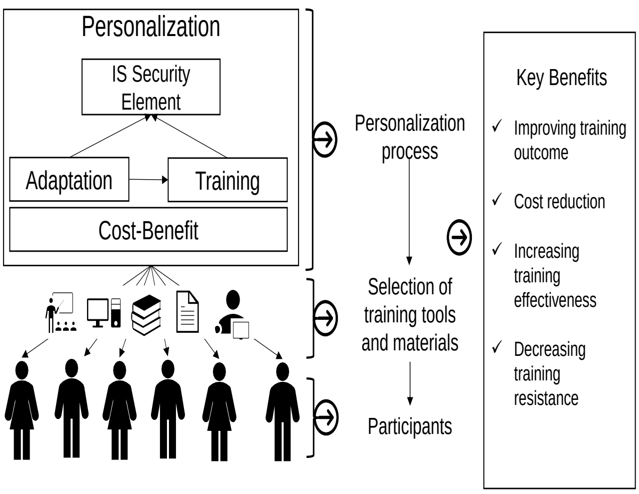

Figure 1. Theoretical foundations of personalized information systems security training.

The IS security training is adapted to the needs of IS users. The proposed approach for personalized IS security training is based on a cost-benefit analysis. The cost-benefit analysis is a tool that helps decision-makers deciding whether to implement a new technology or service. It tries to determine if some investment in the present pays off in the future. A key concept of the cost-benefit analysis is Net Present Value (NPV):

$$NPV = -K + \sum_{t=0}^{T} \frac{R_t - C_t}{(1+i)^t} \quad (1)$$

K is the value of an investment at present (time 0), t is a certain point of time of an investment, R_t is the benefit return of an investment and C_t are ongoing costs at t, and i is the discount rate [29]. The ideal *NPV* is positive or greater than zero. If most investments have a *NPV* greater than zero, prioritization of investments can be done (e.g., by implementing investments with the highest *NPV*) [29]. The cost-benefit analysis therefore enables the identification of an optimal IS security solution and its most effective implementation by gaining an insight into what which IS security elements are worthwhile and effective, and which are not. Overall, the personalization of IS security aims to reduce the costs of training, increase the motivation of participants for engaging in IS security training, and thus maximize the IS security training effectiveness.

We provide illustrative examples for demonstrating the value of the traditional (one-size-fits-all) training approach (NPV_{trad}), and the personalized training approach (NPV_{per}). Let's imagine that a company with 700 employees wants to train them in information security. Our calculations are based on the European Union (EU) average hourly rate (€ 28) [26], costs of traditional training (€ 10 per hour) [15], and average costs of a data breach (€ 3,000 per employee) [9]. We predict that costs of personalized training can be up to 50 percent higher than regular training (€ 15 per hour). C_t is calculated based on absenteeism costs (employees are absent from work due to training) and training costs. We assume that employees are absent for 5 hours during traditional training, and on average 2 hours during personalized training since they attend only training that is relevant for them. R_t is similar for both approaches as employees learn how to prevent and react in the case of a security accident. We assume that without proper security training there would be a data breach once every four years costing € 2,100,000. If security training is fully effective in preventing data breaches, its R_t is equal to average data breach costs per year (€ 525,000). K is calculated based on the average hourly rate. We assume that 2 hours are spent on the development of each personalized training (€ 39,200), while 16 hours are spent on preparation of traditional training (€ 448). Since it is not relevant for the purposes of these illustrative examples, we assume that i is 0. Finally, we assume T is 3 meaning that we carry out three security training sessions per year.

Based on the above assumptions, we can calculate NPV_{trad}, and NPV_{per} per year as follows.

$$NPV_{trad} = -448 + \sum_{t=1}^{3} \frac{175{,}000 - 133{,}000}{(1+0)} \quad (2)$$

$$NPV_{per} = -39{,}200 + \sum_{t=1}^{3} \frac{175{,}000 - 60{,}200}{(1+0)} \quad (3)$$

The results demonstrate that NPV_{per}=€ 305,200 is considerably more cost effective than NPV_{trad}=€ 125,552.

4.2. A Personalized Information Systems Security Training Approach

The proposed approach is composed of five phases:

1. Identification of generic IS security elements.
2. Identification of case-specific IS security elements.
3. Evaluation of case-specific IS security elements.
4. IS user profiling.
5. Adaptation of IS security training as presented in Figure 2.

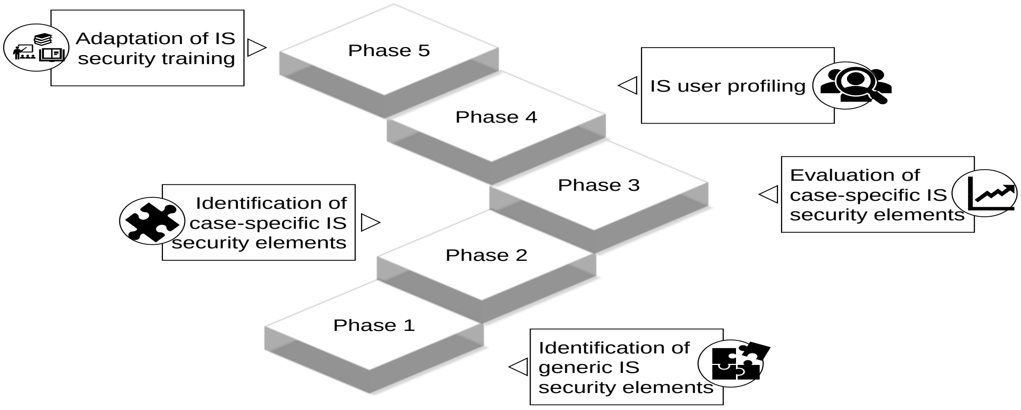

Figure 2. The proposed personalized information systems security training approach.

Identification of generic IS security elements involves the identification of generic IS security elements from cyber and information security bodies of knowledge. This phase aims to build a comprehensive list of necessary IS security elements for both personal and business use of IS with the purpose of getting an overview of all potential IS security elements. This enables distinguishing between basic (i.e., all organization employees need them) and specialized (i.e., at least some employees need them, or they are outsourced) IS security competencies. A survey of both scientific and professional literature is needed in this phase. The key result of this phase is a list of generic IS security elements. The list needs to be regularly updated as IS security is a rapidly changing field.

Identification of case-specific IS security elements represents a logical upgrade of the first phase. It aims to identify the most relevant and important IS security elements for a specific IS. Interviews and/or surveys with all relevant stakeholders (e.g., information security officers, IT managers, system administrators) are needed to exclude non-important IS security elements and potentially identify elements that are not on the general IS security elements list.

Evaluation of case-specific IS security elements aims to assess the identified case-specific IS security elements from various perspectives determined as important by the key stakeholders. It provides the needed empirical grounds for the adaptation of IS security training based on IS security elements. For example, IS security elements are evaluated from technological (e.g., the impact of an element on the overall IS security), knowledge (e.g., IS users' knowledge), behavioral (e.g., motivation of IS users to adequately use the element), or financial (e.g., training costs) viewpoint. Important dimensions of IS security elements are evaluated in a survey. Different stakeholders may be able to provide data for different perspectives. For example, system administrators may evaluate IS security elements from the technological viewpoint and training costs associated with them may be evaluated by the IT management.

IS user profiling aims to build profiles of (potential) IS security training participants by gathering various data on them (e.g., IS security knowledge, IS security value, preferred learning styles). A variety of methods, such as surveys, interviews, and studying IS and organizational documentation, can be used to gather the relevant quantitative and qualitative data on IS users. Heuristic strategies are used for analyzing collected data resulting in recommendations for improvement of IS security training.

Adaptation of IS security training aims to leverage the results of evaluation of case-specific IS security elements and IS user profiling to develop personalized training approaches. The training unit can be either an individual IS user (e.g., high-value IS user) or a group of IS users (e.g., IS users with similar IS security training needs and learning styles). The effectiveness of the adapted IS security training needs to be evaluated (e.g., knowledge gain, costs, participant satisfaction) to provide a feedback loop enabling its continuous improvement.

The proposed IS security training approach can be applied in an organization ad hoc as needed or introduced as a continuous process. However, it can deliver the most benefits due to process optimization only in the latter case. Process capability maturity models including cybersecurity capability models can be used as a benchmark to evaluate the current level of IS security training and its processes, and help setting goals and priorities for its improvements [18].

5. Conclusions

5.1. Possible Applications

Personalization is a concept that has been known in IS research for decades and is used to tailor processes and/or products to the specific needs of their users. In IS security, personalization has emerged only recently. A lot of effort is being invested in improving and finding ways to customize IS security training that would help the participants to achieve better learning outcomes and reduce the costs. The proposed approach for personalized IS security training is based on adapting both IS security elements and the training approach itself.

A key advantage of the proposed approach is its scalability. It can be used in very large companies with thousands of employees. In such settings, the training costs may be lowered due to executing training only for the important IS security elements and only for the participants that need it. Since IS security training may be needed continuously in such settings, IS security training process optimization would be beneficial and could further lower the costs of continuous IS security training. Even if IS security training is needed only periodically (e.g., medium and small companies), there are still several benefits of personalization besides training costs reduction related to focusing on important IS security elements only. The effectiveness of the training (e.g., better training outcomes, higher participant satisfaction) is ensured by IS user profiling which may also lower the user resistance to participation in IS security training as a side-effect. Although technology form the base of IS security, IS users are one of the key attack vectors for compromising an IS. Therefore, IS user profiling also enables companies to evaluate their current IS security level from the user perspective.

5.2. Limitations and Future Work

There are numbers of limitations and directions for future work that the reader should note when interpreting our work. First, this paper formulates a novel IS security training approach and discusses its implications and potential applications. Studies of applying the proposed approach in practice would be beneficial to support the ecological validity of the proposed approach. Second, future studies may focus on individual parts of the proposed approach, such as approaches for identifying case-specific IS security elements and evaluating them, or IS user profiling and building recommender systems. Third, comparative studies of personalization IS security training approaches may be beneficial although difficult to conduct in real-world scenarios. Fourth, physiological measurements [12] in learning could yield interesting results.

References

[1] Aldawood H. and Skinner G., "Reviewing Cyber Security Social Engineering Training and Awareness Programs-Pitfalls and Ongoing Issues," *Future Internet*, vol. 11, no. 3, pp. 73, 2019.

[2] Alfoudari A., Durugbo C., and Aldhmour F., "Understanding Socio-Technological Challenges of Smart Classrooms Using A Systematic Review," *Computers and Education*, vol. 173, pp. 104282, 2021.

[3] Choi S., Martins J., and Bernik I., "Information security: Listening to the Perspective of Organisational Insiders," *Journal of Information Science*, vol. 44, no. 6, pp.752-767, 2018.

[4] Coenraad M., Pellicone A., Ketelhut D., Cukier M., Plane J., and Weintrop D., "Experiencing Cybersecurity one Game at a Time: A Systematic Review of Cybersecurity Digital Games," *Simulation and Gaming*, vol. 51, no. 5, pp. 586-611, 2020.

[5] Deng Y., Lu D., Chung C.J., Huang D., and Zeng Z., "Personalized Learning in a Virtual Hands-on Lab Platform for Computer Science Education," *in Proceedings of IEEE Frontiers in Education Conference*, San Jose, pp. 1-8, 2019.

[6] Ding Y., Meso P., and Xu S., "A Theoretical Model for Customizable Learning/Training to Ehance Individuals' Systems Security Behavior," *in Proceedings of Americas Conference on Information Systems*, pp. 1-8, 2015.

[7] Dorobăt I. and Năstase F., "Personalized Training in Romanian SME's ERP Implementation Projects," *Informatica Economica Journal*, vol. 14, no. 3 pp. 116-127, 2010.

[8] Ellatif M., Salama S., Helmy Y., and Ouf S., "Semantic Web based Algorithm for Personalized Learning Environment," *International Journal of Computer Science and Information Security*, vol. 5, no. 6, pp. 86-107, 2016.

[9] ENISA., "Threat Landscape 2020-Data Breach," Technical Report, 2020.

[10] Fan H. and Poole M., "What is Personalization? Perspectives on the Design and Implementation of Personalization in Information Systems,"

Journal of Organizational Computing and Electronic Commerce, vol. 16, no. 3, pp. 179-202, 2006.

[11] Fujs D., Vrhovec S., and Vavpotič D., "Bibliometric Mapping of Research on User Training for Secure Use of Information Systems," *Journal of Universal Computer Science*, vol. 26, no. 7, pp. 764-782, 2020.

[12] Geršak V. and Geršak G., "Wearables in the classroom-Psychophysiology in Education," *Elektrotehniski Vestnik/Electrotechnical Review*, vol. 88, no. 3, pp. 113-120, 2021.

[13] Ghafir I., Saleem J., Hammoudeh M., Faour H., Prenosil V., Jaf S., Jabbar S., and Baker T., "Security Threats to Critical Infrastructure: the Human Factor," *Journal of Supercomputing*, vol. 74, no. 10 pp. 4986-5002, 2018.

[14] He W. and Zhang Z., "Enterprise Cybersecurity Training and Awareness Programs: Recommendations for Success," *Journal of Organizational Computing and Electronic Commerce*, vol. 29, no. 4, pp. 249-257, 2019.

[15] House N., "The Complete Cyber Security Course : Hackers Exposed!," (UDEMY). Volume1: Become a Cyber Security Specialist, Learn How to Stop Hackers, Prevent Hacking, Learn IT Security and INFOSEC, Last Visited, 2021.

[16] Katsantonis M., Fouliras P., and Mavridis I., "Conceptual Analysis of Cyber Security Education Based on Live Competitions," *in Proceedings of IEEE Global Engineering Education Conference*, Athens, pp. 771-779, 2017.

[17] Mangaroska K., Vesin B., and Giannakos M., "Elo-Rating Method: Towards Adaptive Assessment in E-Learning," *in Proceedings of IEEE 19th International Conference on Advanced Learning Technologies*, Maceio, pp. 380-382, 2019.

[18] Rea-Guaman A., San Feliu T., Calvo-Manzano J., and Sanchez-Garcia I., "Comparative Study of Cybersecurity Capability Maturity Models," *in Proceedings of International Conference on Software Process Improvement and Capability Determination*, Palma de Mallorca, pp. 100-113, 2017.

[19] Reichelt M., Kämmerer F., Niegemann H.M., and Zander S., "Talk to me personally: Personalization of language style in computer-based learning," Computers in Human Behavior, vol. 35, pp. 199-210, 2014.

[20] Sedkaoui S. and Khelfaoui M., "Understand, Develop and Enhance the Learning Process with Big Data," *Information Discovery and Delivery*, vol. 47, no. 1, pp. 2-16, 2019.

[21] Tabash M., Abd Allah M., and Tawfik B., "Intrusion Detection Model Using Naive Bayes and Deep Learning Technique," *The International Arab Journal of Information Technology*, vol. 17, no. 2, pp. 215-224, 2020.

[22] Troussas C., Krouska A., and Sgouropoulou C., "Collaboration and Fuzzy-Modeled Personalization for Mobile Game-Based Learning in Higher Education," *Computers and Education*, vol. 144, pp. 103698, 2020.

[23] Vasileiou I. and Furnell S., "Enhancing Security Education Recognising Threshold Concepts and Other Influencing Factors," *in Proceedings of the 4th International Conference on Information Systems Security and Privacy*, Madeira, pp. 398-403, 2018.

[24] Vasileiou I. and Furnell S., "Personalising Security Education: Factors Influencing Individual Awareness and AC," *in Proceedings of ICISSP-Information Systems Security and Privacy: 4th International Conference*, Madeira, pp. 189-200, 2018.

[25] Vavpotič D., Žvanut B., and Trobec I., "A Comparative Evaluation of E-Learning and Traditional Pedagogical Process Elements," *Educational Technology and Society*, vol. 16, no. 3, pp. 76-87, 2013.

[26] "Wages and Labour Costs," https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Wages_and_labour_costs, Last Visited, 2021.

[27] Wang D., Han H., Zhan Z., Xu J., Liu Q., and Ren G., "A Problem Solving Oriented Intelligent Tutoring System to Improve Students' Acquisition of Basic Computer Skills," *Computers and Education*, vol. 81, pp. 102-112, 2015.

[28] Yamin M., Katt B., and Gkioulos V., "Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture," *Computers and Security*, vol. 88, pp. 101636, 2020.

[29] Zeng W., "A Methodology for Cost-benefit Analysis of Information Security Technologies," *Concurrency Computation: Practice and Experience*, vol. 31, no. 7, 2019.

[30] Zhang J., Guo Y., and Chen Y., "Collaborative Detection of Cyber Security Threats in Big Data," *The International Arab Journal of Information Technology*, vol. 16, no. 2, pp. 186-193, 2019.

Damjan Fujs is Assistant and Ph.D. student at the Faculty of Computer and Information Science, University of Ljubljana, Slovenia. His research interests include cyber security, security requirements engineering and software development methodologies.

Simon Vrhovec is Associate Professor at the University of Maribor, Slovenia. His main research interests are in human factors in cybersecurity, secure software development, agile methods, and change management.

Damjan Vavpotič is Associate professor and head of Information Systems Laboratory at the Faculty of Computer and Information Science, University of Ljubljana. While his main area of expertise is in the field of business information systems, in recent years his research also focused on analysis of longitudinal geospatial data in tourism and healthcare. He has published in a range of scientific journals including Business and Information Systems Engineering, International Journal of Project Management, Information and Software Technology, International Journal of Environmental Research and Public Health, and Tourism Economics where he received 2019 Tea Sinclair Award for Article Excellence.