VARSTVOSLOVJE,
Journal of Criminal
Justice and Security,
year 16
no. 2
pp. 117–127

Information Security Related to the Use of Mobile devices in Slovene Enterprises

Blaž Markelj, Igor Bernik

Purpose:

In the business world, mobile devices represent an important tool for carrying out one‘s work. By providing the possibility to have constant access to different types of data and information, such devices are an important element in the decision-making process. The access to necessary data at any given moment in the decision-making process represents a competitive edge in the business environment. However, despite all of the advantages provided by mobile devices, their users fail to consider the issue of information security, since the access to and transfer of information via mobile devices makes them vulnerable to security risks. The media report on numerous new threats that put mobile devices at risk on a daily basis. The realisation of such threats to information security becomes more likely when users use mobile devices carelessly and simultaneously fail to use adequate security protection. It is therefore important for organisations and experts responsible for the safe use of mobile devices to introduce appropriate technical and organisational solutions and measures for the safe use of such devices.

Design/Methods/Approach:

Conclusions are based on descriptive findings and results of a study conducted among the staff of different Slovene organisations, who are responsible for the safe use of mobile devices by employees.

Findings:

Users of mobile devices in different organisations use their devices both for private as well as for business purposes, and the use of such devices gives them a competitive edge in the business world. Results of a study conducted in 34 Slovene organisations demonstrate that these organisations are currently in the initial stages of introducing both technical and organisational solutions, and measures for the provision of information security related to the use of mobile devices among their employees. According to the findings, the use of regulations and standards, which would define the safe use of mobile devices in relevant organisations, is rare. In mobile devices, the boundary between personal and business data has disappeared completely. The use of mobile devices must, therefore, follow the information security recommendations and provide adequate protection of data accessible to users.

Research Limitations/Implications:

The topic discussed in this paper remains a sensitive issue for different organisations, which is why conducting the study was rather challenging. The number of existing research efforts in this field is limited, and consequently, there are very few grounds that could serve as the basis for the performance of the aforementioned research.

Practical Implications:

Results show the manners in which mobile devices are used and protected against threats. On the basis of these results, organisations could seek ways to improve their methods for the protection of mobile devices and increase the level of protection awarded to their information systems.

Originality/Value:

Work conducted in the field of mobile devices is original and deals with the issues presented hereby in an innovative manner.

UDC: 004.056:[004.382.75+621.395.721.5]

Keywords: mobile devices, threats, security, organisations, Slovenia

Informacijska varnost ob rabi mobilnih naprav v slovenskih podjetjih

Namen prispevka:

Mobilne naprave so v poslovnem svetu pomemben delovni pripomoček. Z možnostjo neprestane povezave do podatkov tovrstne naprave predstavljajo pomemben element v procesu odločanja. Dostop do potrebnih podatkov v trenutku odločanja v poslovnem svetu pomeni konkurenčno prednost. Poleg vseh prednosti, ki jih mobilne naprave ponujajo, pa uporabnik malo razmišlja o informacijski varnosti, saj z dostopanjem in prenosom informacij z mobilnimi napravami le-te izpostavljamo varnostnim tveganjem. V medijih vsakodnevno beremo o številnih novih grožnjah, ki pretijo omenjenim napravam, kar pa ob uporabnikovi nevestni rabi in hkratni neuporabi varnostnih zaščit predstavlja verjetnost za uresničitev groženj informacijski varnosti posameznika in/ali organizacije. Zato je pomembno, da organizacije in strokovnjaki, ki so zadolženi za varno rabo mobilnih naprav, vpeljejo ustrezne tehnične in organizacijske rešitve in ukrepe za varno rabo mobilnih naprav.

Metode:

Ugotovitve temeljijo na deskriptivnih dognanjih in izvedenih raziskavah med strokovnjaki v slovenskih organizacijah, ki so odgovorni za varno rabo mobilnih naprav med zaposlenimi.

Ugotovitve:

Uporabniki mobilnih naprav v različnih organizacijah uporabljajo mobilne naprave tako v zasebne kot v poslovne namene, njihova raba pa predstavlja kokurenčno prednost v poslovnem okolju. Rezultati raziskave, izvedene v 34 slovenskih organizacijah, kažejo, da so organizacije v začetnih fazah uvajanja tako tehničnih kot organizacijskih rešitev in ukrepov za vzpostavitev informacijske varnosti ob rabi mobilnih naprav med zaposlenimi. Uporaba pravilnikov in standardov, ki bi opredeljevali varno rabo mobilnih naprav v organizacijah je redkost. Pri tem pa je meja med osebnimi in poslovnimi podatki na mobilnih napravah popolnoma izginila, zato je pri njihovi rabi nujno slediti informacijskovarnostnim priporočilom in zagotoviti ustrezno zaščito podatkov, do katerih imamo dostop.

Omejitve/uporabnost raziskave:

Tematika, obravnavana v prispevku, je za organizacije občutljive narave, zato je bila izvedba raziskave zahtevna. Tovrstnih raziskav je malo, zato ni veliko osnov, na katere bi se oprli pri izvedbi predstavljene raziskave.

Praktična uporabnost:

Rezultati raziskave kažejo načine rabe mobilnih naprav in zavarovanja le-teh pred grožnjami. Na podlagi rezultatov organizacije lahko pristopijo k izboljšanju načina varovanja mobilnih naprav in dvigu zaščite informacijskih sistemov.

Izvirnost/pomembnost prispevka:

Predstavljeno delo na področju rabe mobilnih naprav je originalno in na izviren način obravnava predstavljeno problematiko.

UDK: 004.056:[004.382.75+621.395.721.5]

Ključne besede: mobilne naprave, grožnje, varnost, organizacije, Slovenija

1 INTRODUCTION

We all live in a period in which one is assumed and expected to make business decisions at any given moment. In this respect, it is of key importance for one to have constant access to business information. Mobile devices[1] enable users in different organisations to be flexible, efficient and respond rapidly. Various networks (Wi-Fi, UMTS, LTE, etc.) allow users to access information pertaining to their organisations, which are stored in a central information system or in a cloud, from anywhere in the world. Some organisations have developed special applications for mobile devices that provide their employees with easy access to the information they need for the performance of their work. The authors of the *IT Spending Priorities Survey 2012*, which saw the participation of 453 information technology experts, attempted to identify projects into which their companies would invest in the following year. A scale of priority projects was then produced. A project related to investments into mobile applications was put

[1] *Mobile devices primarily include devices that use adaptive operating systems, such as iOS, Android, BlackBerry OS or Windows mobile, and are portable (mobile phones, tables, etc.). This category may also contain all devices, which are portable and enable internet access without a physical connection (laptops and other portable computers, game consoles, industrial scanners, etc.), while the group of mobile phones includes both mobile phones intended solely for making phone calls and sending or receiving SMS messages, as well as smart phones, which represent a contemporary communication device, since they not only allow for making phone calls via mobile networks, but also provide a whole range of additional functions similar to those of a PC.*

high on the priority scale (seventh place; 11 percent), while respondents placed a project involving the creation of a central system of control over mobile devices (MDM) on the ninth place (8 percent). The research clearly demonstrated that organisations are extremely interested in investing into mobile devices (Feldman, 2012), which is quite understandable, as trends that have already been observed since 2011 show that the scope of mobile business will increase by 30 percent by 2013 (Mulpuru, Evans, Sehgal, Ask, & Roberge, 2011). This share has been increasing consistently, and in addition, software used in mobile devices has been developing at an extremely rapid pace (Hurlburt, Voas, & Miller, 2011; Oppenheim, 2010), with the purpose to attract the users (Greene, Tamborello, & Micheals, 2013) and increase sales. However, users tend to overlook the dangers they are exposed to in cyberspace when using mobile devices. At the same time, they do not provide for the protection that would enable them to avoid the pitfalls present in cyberspace. This is also supported by the Ponemon Institute's (2012) research dedicated to the identification of risks generated in organisations and posed by mobile devices and information infrastructure used by end users. Seventy percent of respondents stated that mobile devices pose the highest risk for the security of information technology and systems in organisations. The aforementioned research also contains a historical comparison of data, which shows that the same response was provided by a mere 9 percent of respondents in 2010 and 48 percent in 2011. The second most important risk in the 2012 research was attributed to mobile applications of unknown origin (67 percent of respondents), which clearly indicates the continuous increase in the number of those who do not perceive mobile devices merely as a means of but also as a threat (security risk) to information technology.

Mobile devices may become targets of software and applications, which are installed in the device in an uncontrolled manner, such as malware and other threats (e.g. spyware, botnets, Bluetooth connection and contamination originating in online social networks (Leavitt, 2011)). The Juniper Networks Report (2011) shows that 85 percent of users have ineffective mobile phone protection, as (some) manufacturers of software for mobile devices allow for the installation of the so-called »back door«, which enables them to manage software settings on a mobile device without the users‘ knowledge, obtain data regarding location, which are automatically submitted by the mobile device (e.g. GPS location), or take control over the mobile device, etc. These trends were also confirmed in the 2013 Report (Juniper Networks, 2013), which was compiled on the basis of a one-year continuous monitoring of the development and occurrence of threats to mobile devices and demonstrated that the quantity of malware has increased by 614 percent between March 2012 and March 2013. The lack of knowledge related to the functioning of mobile devices' software and different functionalities that it provides cause users to become targets of cybercrime. The awareness of threats and their implications, which may put the users of mobile devices at risk, is also important in order to become aware of the need to provide sufficient cyber security.

In order to determine the actual state-of-affairs in this field, the authors of this paper conducted a study of Slovene organisations, during which the persons responsible for the safe use of mobile devices among employees were asked about the manners in which their employees use mobile devices and the methods applied to provide information security. The objective of the research was to obtain information about the possibilities of introducing and using different technical and organisational protective measures related to the use of mobile devices among employees of individual organisations.

2 METHODS

The research was conducted through interviews, with representatives (responsible for the safe use of mobile devices) of 34 organisations completing a questionnaire via e-mail. Twenty-two completed questionnaires were (also via e-mail) sent back to the researchers. When devising open-ended leading questions (19 questions), the researchers followed theoretical premises related to the use of mobile devices, thus stimulating individual respondents to share their experience in and views on the use of mobile devices in their organisations.

Since the research was dedicated to the ways of conducting security-related activities and formal responsibility, the aim of the researchers was to verify *who was in charge of mobile devices in an organisation and was thus formally responsible (for their security, the selection of models, education and training, etc.).* Responsibilities in the field of mobile devices were most often (40.9%) assumed by ICT departments (information and communication technologies), which is reasonable, as they are familiar with the structure of the IS (information system) and the storage of data, the provision of security and the structure of their organisations. In 31.8 percent of organisations included in the research, several departments within the organisation are in charge of mobile devices (IT department, security department, head of information security and protection, etc.). Organisations are aware of broader issues related to the complexity of the provision of information security for mobile devices and strive to fully meet security criteria in this field, which is why they often involve several departments specialised in different fields of expertise. In 9.1 percent of these organisations, persons in charge of mobile devices work in departments responsible for quality assurance and projects or in general affairs departments. 18.2 percent of organisations leave the responsibility for mobile devices to the employees themselves or do not dedicate any particular attention to this issue. The ways in which organisations provide for the security of devices are presented below.

3 RESEARCH

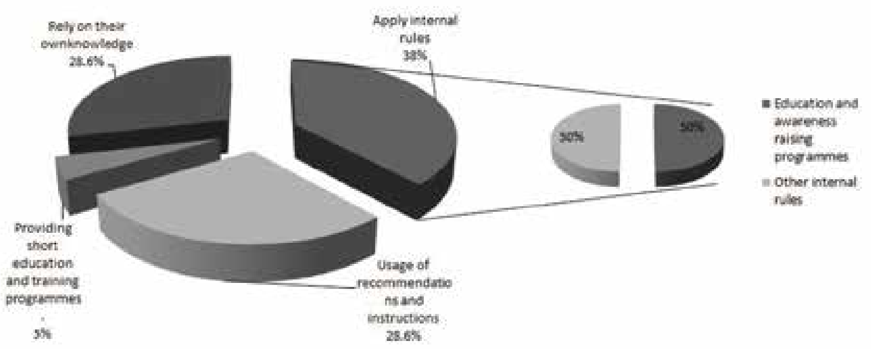
Information regarding the methods used for providing security were obtained by posing the following question: *How does your organisation arrange for the safe use of mobile devices (e.g. regular education and training programmes for users, introduction of standards, etc.)?* Responses were grouped to reflect the following four groups of organisations, which:

- provide for the safe use of devices through security policies and internal rules,
- implement instructions and recommendations to guarantee security,

- raise the security awareness of users by providing education and training, and
- leave security related activities in the hands of individuals without exercising any type of control and are not aware of the threats to information systems and the integrity of data generated by the use of mobile devices.

Researchers also observed the formation of a group of organisations, which do not only use internal rules and regulations but also provide education and awareness raising programmes for users, thus providing adequate measures for the safe use of mobile devices. The above question was answered by 21 organisations (*n* = 21) as shown on Figure 1.

Figure 1: How does your organisation arrange for the safe use of mobile devices (e.g. regular education and training programmes for users, introduction of standards, etc.)?



This means that 38.6 percent of organisations, i.e. 8 organisations, apply internal rules defining the use of mobile devices. At the same time, 4 (50%) organisations (from 8 organisations) also provide their employees with education and awareness-raising programmes for the safe use of mobile devices in addition to the implementation of internal rules. The group of organisations, which define the use of mobile devices through recommendations and instructions, is composed of 6 organisations. One organisation guarantees the safe use of mobile devices among their employees merely by providing short education and training programmes. Six organisations have not (yet) devised a systematic method for the use of mobile devices, which is why their employees are left to their own devices and have to rely on their knowledge regarding appropriate conduct.

Responses to the next question: *What kinds of procedures does your organisation apply to allow users to use their own mobile devices for work purposes and access to the business environment?* fall within two groups. The first group is composed of 16 organisations (72.8%) that apply a particular procedure defining the use of users' own mobile devices. The second group consists of 6 organisations (27.2%), which do not allow users to use their own mobile devices for work purposes and consequently do not apply any specified procedures to this end. The ways in which an organisation may prescribe the use of users' own devices for access to business systems can be of a technical (a mobile device becomes part of the MDM or MAM tools used in an organisation) (Goldman, 2012) or an organisational nature. MDM tools (Mobile Device Management) focus on exercising control over a mobile device as a whole (Citrix, 2014; Kwon & Kim, 2013), while MAM tools (Mobile Application Management) control a mobile device on the level of individual applications (Keen, 2013; Murray, 2012). The exercise of control depends on the introduction of organisational measures and adequate rules defining the use of mobile devices in an organisation and prescribing procedures for their use, including or primarily in terms of security solutions.

In order to ascertain whether organisations regulate the use of mobile devices by adopting specific acts, respondents were asked the following question: *Does your organisation have any specific rules concerning the safe use of mobile devices? Which security elements do they contain?* Four (18.2%) organisations adopted rules regulating the safe use of mobile devices, but on the other hand, the fact that 18 (81.8%) organisations do not apply and rules regarding the safe use of mobile devices raises serious concern.

The level of awareness and the implementation of cyber security procedures were ascertained by posing the following question: *How does your organisation raise awareness of users regarding the safe use of mobile devices? Please list the methods and evaluate the time spent for implementing an individual method.* This question was answered by 21 respondents (*n* = 21). One organisation has never conducted education or training courses for its employees, while 20 organisations responded that they train and raise awareness of their employees regarding the safe use of mobile devices in different ways, e.g. through different memos and information provided via their intranet and internet sites, by organising training programmes for groups of employees or by providing training courses for individuals when these receive a new mobile device, etc. The time organisations dedicate to such education and training activities differs significantly, ranging from 15 minutes per month, three hours per year, one day per year or even two days per month (when this research was conducted, some organisations were in the middle of an intense process for the provision of a higher level of security of their mobile devices). Naturally, the quantity of education and training activities also depends on individual employee's position in the organisation and/or the general provision of cyber security and educational methods (individual or group training, education via the internet, etc.).

When analysing responses to the question regarding procedures applied in case of abuse *(What kind of procedures does your organisation foresee in the event of abuse of information sources via users' mobile devices?)*, the situation varies greatly. Two organisations (9.1%) have not defined any procedures for dealing with abuse, while others (90.9%) would initially consider such abuse as a security incident and then take appropriate steps in line with policies, instructions or guides to good practice adopted by their organisations. They would most often inform the person responsible for security incidents in the organisation, followed by the implementation of a standard procedure foreseen in such cases. None of the organisations concerned has adopted a special procedure to be applied in the event of an abuse of information sources via mobile devices. This means that they use general rules related to security incidents. In the event of abuse, only one organisation would act in line with the legislation and internal rules, and would simultaneously report the incident to the police.

The aim of the following question: *What kinds of responsibilities and powers are attributed to the users of mobile devices?* was to ascertain whether organisations encourage users to use mobile devices in a safe manner, provided they previously attended adequate education and training courses. Some organisations define the responsibility of mobile devices' users in the framework of other rules and regulations (e.g. access to different types of information, password handling and management, handling of computer hardware and software, etc.), while others use general provisions concerning responsibility.

4 DISCUSSION

In organisations, the responsibility for the safe use of mobile devices is mostly attributed to a person who is in charge of information security and, at the same time, possesses appropriate competences and knowledge required to deal with mobile devices. This task combines different aspects that have to be included in order to meet the criteria for the safe use of mobile devices. Those organisations, which provided such a response, are aware of the breadth and complexity of the issue. In some organisations, the safe use of mobile devices is entrusted to those persons or departments that have no background in the field of information security, which is why it is difficult to predict how exactly do they manage to perform their regular daily tasks and simultaneously deal with the rapidly developing/changing and ever more complex field of mobile device security. One may even ask whether they possess adequate knowledge and skills required to do so. With respect to the safe use of mobile devices, the share of organisations (28.6%), in which the manner of using mobile devices and handling data is left to individual users, who may apply completely different practices, which results in an array of methods and ways of using mobile devices within an individual organisation, is alarming. At the same time, one may ask what is the level of knowledge they possess, if any, regarding the safe use of mobile devices. Other groups of organisations are currently developing procedures, which is why it is expected that this field will (mostly) be appropriately regulated in the future.

Procedures allowing the use of one's own mobile device for work or business purposes are defined in an organisations' internal rules, and such procedures are mostly specifically defined. Procedures are initially most often conducted by adopting the view that users may use their own mobile device(s) for work purposes, while the adequate application form is processed by a person responsible for security at a later stage. The responsible person considers the authorisation for and the extent of the use of a device, the implementation of protective measures and security features, and the access to information on the basis of defined methods and criteria that have to be met in order for the user to be able to use a personal mobile device for work or business purposes. Rules that define the safe use of mobile devices mostly contain the following sections:

- steps to be taken in the event of a loss or theft of a mobile device,
- conduct in the event of accessing the internet via public hotspots,
- safe access to the organisation's information system.

None of the organisations involved in the research stated that their internal rules contain a provision which would ban or restrict the use of software that has not been authorised by the organisation concerned. This represents a serious deficiency given the vast amount of different software applications that are accessible via mobile devices and are often the cause of information loss (Josyula, 2013). It is, therefore, vital to take this into account and complement existing internal rules with a section which would contain a detailed breakdown of individual rules and measures, in order to provide for a suitable level of cyber security. With respect to the methods used to raise awareness of users regarding the safe use of mobile devices and cyber security, researchers find that education and training activities are mostly conducted via e-mail memos or information provided via internet sites. Such memos and information are mostly of a general nature, while some organisations occasionally inform their employees about threats when they come across reports about the increased level of threats, and consequently the amount of security incidents, via the internet or in the media. All organisations agree that rules and standards contribute to an increased safety of processes in the organisation, but they add that there is a lot of room for improvement in the field of general awareness raising among users with respect to cyber security, threats and consequences of mobile devices' abuse. In addition, individual elements defined in standards and rules should be more consistently implemented. In case organisations detect the abuse of information sources via a mobile device, they mostly adhere to the prescribed general procedure for security incidents, which is most often conducted through the following steps:

- report of the incident to the responsible person,
- opening of the security incident document,
- identification of the cause and its remedy,
- identification of consequences and their evaluation,
- damage assessment, and
- potential sanctions, provided that these were previously defined and are justified from the point of view of other circumstances affecting the situation.

It is vital to complement the above procedure with actions stemming from internal acts, which are implemented and in line with the legislation, and with the need to report incidents to national authorities, such as the Slovene Computer Emergency Response Team (SI-CERT) and the Police or the national cyber security centre, where such centre exists (a proposal concerning its establishment is currently being discussed in the Republic of Slovenia). Organisations, apart from those that have explicitly defined the provisions related to authorisations and responsibilities, generally do not define any specific provisions, which means that general rules apply for all users of mobile devices.

The responsibility for the safe use of mobile devices and the manner in which these are used are often left in the hands of individual users and their own judgment regarding the sound management of devices and processes. At the same time, organisations presume (often erroneously) that users are aware of security concerns. However, given the trends related to the increasing growth in the number of threats and ever more complex requirements for maintaining a sufficient level of information security, this is simply unacceptable. Information security of an individual organisation is as strong (protected) as its weakest link, i.e. the user of a mobile device, the device itself, and the access to the comprehensive information system of an organisation. It is, therefore, inappropriate to leave decision-making regarding information security to individual users of mobile devices, who mostly do not possess adequate knowledge and are not willing to encroach upon their own rights for the sake of information security. Decisions regarding information security must be taken by the organisation and persons, who possess adequate knowledge, while the rules regarding the safe use of mobile devices must be introduced into the organisational environment through internal rules and standards.

REFERENCES

Citrix. (2014). *XenMobile*. Retrieved from http://www.zenprise.com/solutions/MDM

Feldman, J. (April 30, 2012). Research: 2012 IT spending priorities survey. *InformationWeek*. Retrieved from http://reports.informationweek.com/abstract/83/8816/it-business-strategy/research-2012-it-spending-priorities-survey.html

Goldman, C. (2012). *What's the difference between MAM and MDM?* [Video]. Retrieved from http://www.apperian.com/mam-mdm/

Greene, K. K., Tamborello, F. P., & Micheals, R. J. (2013). Computational cognitive modeling of touch and gesture on mobile multitouch devices: Applications and challenges for existing theory. In M. Kurosu (Ed.), *Human-computer interaction: Interaction modalities and techniques* (pp. 449–455). Heidelberg: Springer.

Hurlburt, G., Voas, J., & Miller, K. W. (2011). Mobile-app addiction: Threat to security? *IT Professional, 13*(6), 9–11.

Juniper Networks. (2011). *Malicious mobile threats report 2010/2011*. Retrieved from http://www.juniper.net/us/en/dm/interop/go

Juniper Networks. (2013). *Juniper Networks third annual mobile threats report.* Retrieved from http://www.juniper.net/us/en/local/pdf/additional-resources/3rd-jnpr-mobile-threats-report-exec-summary.pdf

Josyula, R. (2013). Application security in mobile devices using unified communications. V N. Meghanathan, D. Nagamalai, & N. Chaki (Eds.), *Advances in computing and information technology* (pp. 135–143). Berlin: Springer.

Keen, M. (January 10, 2013). *Got MAM (mobile application management) in your 2013 mobile menu?* Retrieved from https://www.ibm.com/developerworks/mydeveloperworks/blogs/mobileblog/entry/got_mam_mobile_application_management_in_your_2013_mobile_menu25?lang=en

Kwon, H., & Kim, S. H. (2013). Efficient mobile device management scheme using security events from wireless intrusion prevention system. In Y. H. Han, D. S. Park, W. Jia, & S. S. Yeo (Eds.), *Ubiquitous information technologies and applications* (pp. 815–822). Dordrecht: Springer.

Leavitt, N. (2011). *Mobile security: Finally a serious problem?* Largo: University of Maryland. Retrieved from http://www.computer.org/portal/web/computingnow

Mulpuru, S., Evans, P., Sehgal, V., Ask, J. A., & Roberge, D. (July 17, 2011). *Mobile commerce forecast: 2011 to 2016.* Retrieved from http://www.forrester.com/Mobile+Commerce+Forecast+2011+To+2016/fulltext/-/E-RES58616?objectid=RES58616

Murray, A. (June 5, 2012). *Mobile application management (MAM) has put MDM in its place.* Retrieved from http://www.networkworld.com/news/tech/2012/060512-mam-mdm-259877.html

Oppenheim, R. (2010). *The App in the haystack: Steps to finding useful and usable Apps.* Retrieved from http://www.highbeam.com/doc/1G1-245168524.html

Ponemon Institute. (2012). *2013 state of the endpoint.* Traverse City: Ponemon Institute. Retrieved from http://www.ponemon.org/local/upload/file/2013%20State%20of%20Endpoint%20Security%20WP_FINAL4.pdf

About the Authors:

Igor Bernik, Ph.D., Assistant Professor of Information Sciences and the head of the Information Security Department at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. His research fields are information systems, information security, and the growing requirements for information security awareness.

Blaž Markelj, Lecturer of Information Science at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. His research interests include blended threats to mobile devices and information security.