MATEC Web of Conferences **210**, 04041 (2018) https://doi.org/10.1051/matecconf/201821004041
CSCC 2018

Security implications of the personal information environment

Pavel Valášek[1,*]

[1]Tomas Bata University in Zlin, nam. T.G. Masaryka 5555, 76001 Zlín, Czech Republic

Abstract. This article discusses a security in a background of the personal information environment. A role and importance of personal information environment and its security is on the rise due to the increasing inclusion of information and communication technology. In many cases, the focus of conducted studies is on the technological part of the problem. In this article, results of the user-oriented study are presented. The main aim was to establish how users perceive security applications. As a preliminary study, a method of survey was utilized. Gathered data were evaluated using common statistical methods. Results of the study are presented in a suitable form with a consideration of a large variety of answers between users. Results show areas of technology and user disagreements. These established differences will be used as a basis of the future research.

1 Introduction

Today information and using of information is present in almost every area of human activity. This problematics is one of the main influencing factors of technic and social advance of society. When approaching information and information processes a distinction between individual users can be observed. These differences can be attributed to a variety of personal prerequisites of individuals. This characteristic can be influenced for example by the social or economic environment, gained knowledge and skills as well as social or professional groups. Such groups can show certain specifics in the area of information processes. Based on its prerequisites, either consciously or subconsciously, an individual creates a set of elements for information acquirement and other processes. This set of elements can be called *"personal information environment"* (PIE). A schematic illustration of a possible PIE can be seen in Fig. 1. [1, 3, 5]

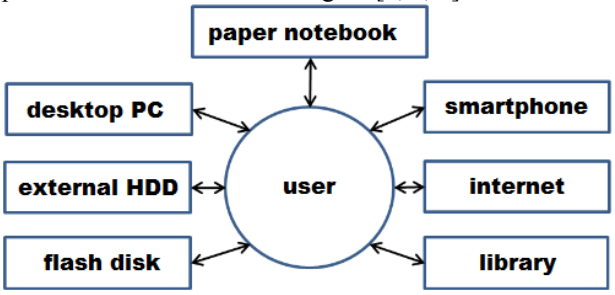

Fig. 1 Schematic illustration of the PIE.

As can be seen in this scheme (Fig. 1) PIE consist of all information sources of users as well as all tools user utilizes to process and archive information. In an accordance with a current development of information and communication technology (ICT), an influence of new technology elements can be observed. The basic idea behind the application of such technologies is to make information processes better and more effective while using large quantities of data. However, for the end-user significance of information for an individual and its activity is more important than information quantity. From a technological point of view, ICT element is included with a purpose of connection stimulation of user on one side and information system, information source and information service on the other side. Implementation of ICT to information processes facilitates easier access to information. In relation to PIE information technology can be considered as a technological means for data and information processing. Communication technology can be viewed as a technology for searching, transferring and accessing information. Elements of both technology types are usually integrated into one device in various forms (personal computer, smartphone). [2, 3, 4]

Similar elements of ICT are integrated among various devices. Despite this, it is hard to determine one type or form of electronic device that would meet all the requirements of a user. Many devices have their specifics of use, rendering them more suitable for a certain group of the user than for the others. Currently, the most used types of devices are various forms of personal computers and various brands and forms of smartphones. The personal computer offers a high variety of possible applications according to requirements of a user. Personal computers are able to operate with a various data formats, suitable for

* Corresponding author: pvalasek@utb.cz

information variability. Their advantage is high computing performance. They have the most computing performance from all the devices that are currently publicly available and commonly used for purposes of the PIE. On the other hand, smartphone type devices are characteristic of their mobility. The modern smartphone is capable of similar tasks as a personal computer while maintaining dimensions of a mobile phone. Smartphone differs from a regular mobile phone in higher computing performance, more advanced functions and larger screen surface and resolution. Personal computers and smartphones are usually used with a technology for storing information. This may take forms from a specialized device (internal or external HDD, optic disc, flash disk) to a complete service (cloud data storages). [6, 7]

As a result of a continuous ICT inclusion into everyday activities and therefore PIE as well security issues are a part of this inclusion. While looking at the structure of individual PIE security reasons should be considered as one of the influencing elements. [8]

The preliminary studies in this area should be conducted to further understand these phenomena. Security of PIE elements is a topic of many studies with a technical point of view, but not many are concerned with a viewpoint of a user. In this context, a data from user feedback of various software cannot be used as it may be biased and does not consider other users. The aim of the conducted study was to explore a posibility of such research.

2 Methods

A broad study was conducted with a general topic of PIE and security questions connected with ICT and PIE. As a part of this study, structured interviews were conducted. Interviews were conducted with a bachelor and master degree students. The students were selected by a means of convenient sampling – a voluntary activity. A previous education concerning ICT wasn't considered.

From the whole sample of 75 students, there were 46 female participants and 29 male participants. The youngest participant was 21 years old; the oldest participant was 24 years old. All of the participants were students of Tomas Bata University in Zlín from various programs.

Interviews were aimed at three main topics – overall opinion on PIE problematics, influence on PIE and protection of PIE. The first topic, overall opinion on PIE problematics, was selected to establish a common ground between interviewer and interviewee concerning PIE – what does respondent understand under this conception, what information processes does respondent encounter and description of respondents PIE. This part of the interview was considerably more moderate than the other stages. This was perceived as necessary for better understanding of the topic on the side of the respondent and to yield better-organized data. Other two topics of conducted interviews are discussed in a Results section.

Due to the character of collected data their evaluation was complicated. Answers in mentioned topics were recorded (written) in a way that allowed further comparison between respondents. The final evaluation consisted of open answer interpretation and subsequent frequency analysis.

The main task of an open answer interpretation was a unification of variable answers under quantifiable keywords. For example questions concerning usage of security elements contained an option "other" with space for the respondent to fill out what other unlisted options does he use. These answers were compared with other answers and their content was analyzed. Repeated answers were considered as a new valid option for said question.

These methods are in compliance with standard methods used for preliminary studies in a field of user feedback.

3 Results

3.1 Influence on PIE

During its work inside PIE, a user is exposed to various factors that can have an influence on the current activity of user as well as the further function of a PIE. These changes can be both positive and negative. From the collected answers two major group could be selected:

- *internal factors*
    - As *internal factors* were considered those that are created inside of the already functioning PIE or, more precisely, are initiated inside the PIE. Most commonly stated *internal factors* were "conscious modification by user" (adding a new device, service…) and "spontaneous PIE changes" (software updates).
- *external factors*
    - Influencing factors initiated outside the PIE itself can be considered "*external factors"*. Users usually stated various forms of advertisement, attacks on personal information and change of PIE forced by the employer. Considering the fact that these factors can lead to loss or theft of information they should be viewed as more dangerous for PIE and information in it.

3.2 PIE protection

Due to the complexity of PIE conception, it is impossible to determine one technology or security approach that could be used for protection of PIE. The impossibility of creating one universal solution for all PIE instances is caused by variability and individuality of users in the area of PIE and information processes altogether. Individual PIEs can be significantly different accordingly to user requirements and PIE focused

protection should reflect this. Depending on a PIE there are differences in protected assets as well as in the structure of individual PIEs. This is the reason why it is insufficient to protect only information itself. The whole PIE should be protected because malfunction of one element can have a negative effect on the element of the PIE and therefore its function. Information can be lost, compromised or became inaccessible to their rightful owner. [9, 10]

When we examined various PIEs of respondents we found out that all examined PIEs contained both elements of ICT as well as more conventional means of information processes such as diary or calendar. Many of the examined PIEs also contained elements that are out of user's control (for example a public server). However, security and protection of such elements are usually handled by according organizations. Considering these elements the main concern of users lays by means of communication with said elements. [5]

During research, there was a vast variety of answers as to what users apply to protect their PIE. For established groups of protection, there are approximate percentages (Fig. 2) of respondents using this approach. Most users apply more than one approach to security and overall PIE protection.

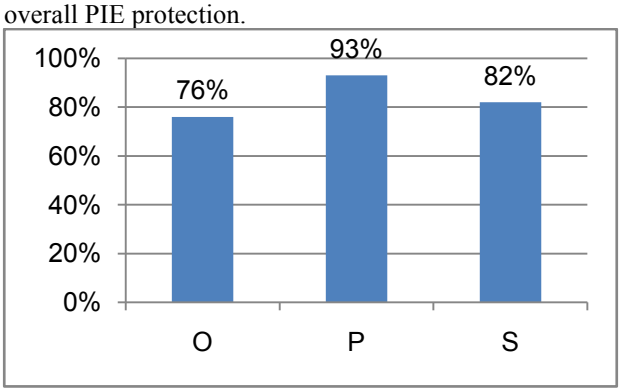

Fig. 2 Approaches to PIE protection by users [%]

3.2.1 Organizational measures (O)

Considering the dependency of PIE on a user we can say that the user is in a certain way an element of protection as well. The activity of the user has the biggest influence on PIE creation and its further function. To properly maintain functionality of PIE it is necessary for a user to abide by certain rules when processing information. These rules depend on the structure of the PIE as well as on the overall information environment of the user. It is up to the user to assess possible threats of social, politic and other "circles" of information environment which its PIE belongs to. Insufficient application of organizational measures can lead to undetected attacks on PIE and its elements. On the other hand, the excessive application may cause the PIE to be unusable or motivate the user to bypass some security measures. [5]

As seen in Fig. 2 around 76% of respondents answered in a way, that implied they use organizational measures to ensure the security of their PIE (column marked "O").

3.2.2 Physical protection (P)

Whether we consider an ICT element included in the PIE or physical non-digital medium their common characteristic is a form of physical representation. In various cases, digital data can be transferred or represented in a physical form. It is contra productive to consider more advanced security measures if the physical access is unrestricted. The user should consider whether his level of physical protection is adequate but also should consider if chosen measures aren't exaggerated – for example: "Is it sensible to buy a safe just to keep a diary?"[11]

The most asked users apply some sort of physical protection. In Fig. 2 (column marked "P") we can see that 93% of asked users protect their PIE on a physical level. Remaining 7% of respondents admitted that they are generally inattentive of their property.

3.2.3 Software protection (S)

As mentioned before one of the most common elements among various PIE instances is some form of personal computer or smartphone. There are both commercial and free-to-use security solutions for these devices. Despite this, in Fig. 2 (column marked "S") we can see that only approximately 82% of asked users were using some of these solutions. This means that shocking 18% of respondents don't use any form of software protection.
Respondents were also asked about a nature of their software protection. Most common answers were:

- antivirus software (A)
- firewall (F)
- proxy server (P)
- other (O)

Respective percentages of respondents can be seen in Fig. 3. Columns are marked with letters (A, F, P, O) presented in a list above.

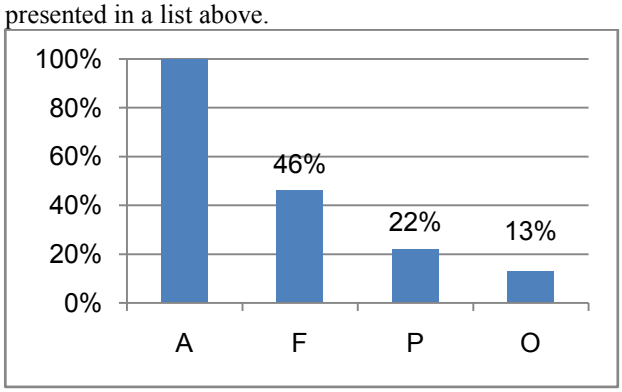

Fig. 3 Software protection users percentages.

4 Discussion

The main aim of this study was to explore possibilities of future research in security perception by users. Findings in this area are necessary for a further advancement in understanding of individual PIEs creation.

As for the general protection of PIE, all asked respondents are aware of security threats and apply one or more kinds of security measures. None of the respondents is unaware of security risks and does not

apply any kind of security measure. It is expected that further studies will confirm this.

It was revealed that physical protection is the most common type of protection. It may be caused by human nature. We are taught to be attentive to our property and this may attribute to a high percentage of users.

The most alarming finding was that approximately 18% of all asked users do not use any form of software protection in general. The further research of this phenomenon could bring answers to why certain users do not feel the need of software protection and what is the influence on the PIE.

Even though PIE itself is unusually the main target of attacks, it is almost always used as a medium of an attack. The risk of attack and its damages can be lowered by a proper protection and suitable security measures. The task is not only mere protection of assets but to create a security system that will consider individuality of a user. It is necessary to develop future security solutions in a way that they will cover current imperfections – methods that are too time-consuming for a user; activities that users see as unnecessary; procedures that user doesn't understand. Even the most technically advanced system working in cooperation with a human element is vulnerable right at this point of interaction with a user.

Phenomena discussed in this article show an evident integration of ICT into a wider spectrum of society as well as it many structures and organizations. The further development of ICT enables easier access to information to people all over the world. It also helps create opportunities for further knowledge advancement in various fields, not only informatics.

The influence of ICT on an academic sphere is undeniable. Many of the ICT advancements were made with science in mind and to connect academic communities all over the world. Acceptance of these technologies into everyday life had a significant economic effect on their further advancement.

One of the main obstacles in ICT development is a human factor, more specifically a variety of differences between individuals. It can manifest itself by inconsistency in approaches to information processes and included technology. Even though many skills and knowledge can be attained it is nearly impossible to secure the same level of these skills and knowledge for every individual. But if we are able to assess groups among users we may be able to create PIE structures that would meet requirements of a certain group of users and still be able to effortlessly share information between such user groups.

PIE problematics seem to be suitable for a selection or assessment of such groups, based on individual, professional or other characteristics. Research of PIE is focused on elements of ICT as well as on users themselves, their demands, requirements, and needs. Suitable analysis of this topic can yield many new findings for various fields such as psychology, ergonomics, management and information management. The most immediately these findings can be applied in software and hardware design.

References

1. P. Valášek, L. Nečesal, *Cybernetics Approaches in Intelligent System; Advances in Intelligent Systems and Computing* **661***;* Springer, Cham (2018)
2. J. Požár, *Manažerská informatika* (2010)
3. L. Lukáš, P. Hrůza, M. Kný, *Informační management v bezpečnostních složkách* (2008)
4. P. Doucek, M. Maryška, L. Nedomová, *Informační management v informační společnosti* (2013)
5. P. Doucek, *Informační management* (2010)
6. J. Vymětal, A. Diačíková, M. Váchová, *Informační a znalostní management v praxi* (2005)
7. P. Toman, *Informatika pro koncového uživatele* (2011)
8. O. Bergman, S. Whittaker, *The science of managing our digital stuff* (2016)
9. W. P. Jones, *Keeping found things found: the study and practice of personal information management* (2008)
10. W. P. Jones, J. Teevan, *Personal information management* (2007)
11. M. Lucki, *Nové trendy v elektronických komunikacích: Moderní zabezpečovací systémy* (2015)