Management,
Knowledge and Learning
International Conference 2012

INDIVIDUAL AND MULTI-USER DIGITAL IDENTITIES OF EMPLOYEES IN POLISH ENTERPRISES – SURVEY RESULTS

Marek Miłosz
Lublin University of Technology, Poland
marekm@cs.pollub.pl

Marta Juszczyk
Lublin University of Technology, Poland
marta.w.juszczyk@gmail.com

Abstract:
Information is one of the crucial factors of business in the globalized world. Access to resources of a company should be easy for employee, allowing efficient performing their duties, but also difficult for unauthorised person. One of the most popular solutions is granting access using pair: login and password. An access to resources of enterprise can be protected in two ways: by creating a digital identity for each employee or for group of employees. Both solutions have specific advantages and drawbacks. The article presents the results of survey conducted in Polish enterprises on usage and perception of these two solutions by employees. Respondents were asked about solution used in theirs companies, their habits and attitude towards digital identity itself, their knowledge about data protection, perceived advantages and disadvantages of individual and multi-user digital identity and their choice of the best solution. The surveys not only allow describing how individual and multi-user digital identities are used, but also indicate critical factors of usage of each type of digital identity.

Keywords: information security, digital identity, human factors.

1. INTRODUCTION

An important aspect of any IT system supporting the work of the company is its safety. Information security is a complex matter. One of its important elements is a control of access of potential users to the system and its functionalities, as well as accountability the activities carried out by particular users. This control involves strictly defined elements: who, when and to what extent should have an access to company resources of information systems (Windley, 2005). This process is implemented in the three areas (Widley, 2005): identification, authentication and authorization of the user.

The significance of identifying entities having access to an application grows in a situation where one employee has to use many applications. Typically, this requires the end user to log on to multiple applications and, consequently, define multiple authentication data (De Capitani di Vimercati & Samarati, 2001). The examples of solutions of this problem are federative identity management systems implementing the idea of "single sign-on" (Maler, 2011; Semančík, 2005).

Regardless of the technical implementation of user authentication, three classical problems can be identified:

- types of permissions (and consequently – authentication of users): individual or for multi-user accounts,
- method of determining and enforcing permissions in practice,
- attitude of users to the identification system and its implementation in practice.

This last problem is important for the security of information across all IT systems. Many authors emphasises the significant influence of human factor on the security of information (Windley, 2005; Shay et al., 2005; Miłosz & Juszczyk, 2010; Maliki & Seigneur, 2007; Juszczyk, 2011).

2. DIGITAL IDENTITY

Digital Identity (DI) is possessed by many entities - from the devices (e.g. RFID tagged), through the companies (e.g. tax number), to the people (Maler, 2011). Human DIs are a critical element of information security system.

DI is used in enterprises to protect computer systems against unauthorized access in a well-understood interest of the company. Depending on the specific application, DI can be individual or multi-user (i.e. group). Individual DI is associated with a single, physical worker. Multi-user DI is related to the role of users performed in IT systems. In this case the role can be performed by many employees.

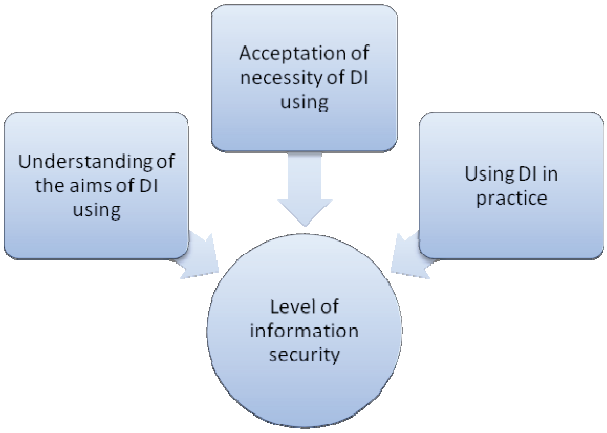
Regardless of the DI type, a typical method of authentication is providing by users of IT systems a pair: username/password. In the paper (Maler, 2011, p. 17) there is a statement: "Most sites rely on username/password pairs because this method poses the smallest initial burden for users and site administrators". This pair combined with other employee's data becomes his or her DI in IT systems of the company.

3. PROBLEM DEFINITION

In the study (Miłosz & Miłosz, 2011) it has been demonstrated that the level of information security in Polish SMEs is insufficient. A large part of Polish SMEs has no Identity and Access Management System (IAMS). A positive aspect of this study was detection that top management knows about IAMSs and profits resulting from their use (Miłosz & Miłosz, 2011).

The proper understanding of the aims, level of acceptance and proper use of DI in practice, both individual and multi-user, have a significant impact on the level of security (Picture 1).

Picture 1: Casual diagram of impact of various human factors associated with DI on information security



4. RESEARCH METHODOLOGY

4.1. Problem formulisation

To assess the level of human factors associated with DI, affecting the security of information systems of enterprises in Poland the following research questions were formulated:

- What is the level of awareness of the aims of applying DI, including the use of individual and multi-user accounts?
- What is the attitude of workers to DI?
- Do employees apply properly the security rules in relation to their DI?

In addition, the study of employee's preferences of the use of individual and multi-user authentication in IT systems was planned.

4.2. Research hypotheses

To verify the research questions following research hypotheses were formulated:

H1. Employees understand the objectives of the DI use; they correctly identify the advantages and disadvantages of individual and multi-user accounts.

H2. Employees have a positive attitude towards DIs. The acceptance increases with the level of employees' knowledge.

H3. Employees of companies correctly apply the safety rules in the area of creating and storing identification data.

H4. Employees prefer individual DI rather than multi-user digital identities.

4.3. Research organisation

The study was conducted in 2011, as a part of work "Acceptance of digital identities in enterprises Lublin Region", realized in the frame of the project "Man - the best investment." The project was funded by European Social Found (ESF).

To verify the research hypotheses there were developed a questionnaire that contained closed questions. Respondents of the survey were 94 employees of large, small and medium enterprises. The representative sample was selected. The sample was also constructed to ensure reflection cross-industry statistics in the region. All the respondents had managerial or administrative positions, and were users of different computer systems of their companies.

5. RESEARCH RESULTS

The results of questions concerning verification of the hypothesis H1 are presented in the Picture 2 and Table 1. Picture 2 shows the percentage of indicated options. Table 1 contains the results of inquiries about the advantages and disadvantages of individual and multi-user DI. Each respondent had to pick up to two options. In the Table 1 there are presented 3–4 top responses, indicated by over 10 % of respondents.

Conclusions from the data presented in the Picture 2 are not clear. Most responses pointed to the need of adaptation to external legal requirements (60 %). Much less respondents indicates the company's data protection or accountability of employees. It allows to draw the conclusion that the use of DI is largely imposed from outside - at least in the minds of employees.

The data in Table 1 indicates the correct identification of the advantages and disadvantages of DI. However the awareness of employees in relation to responsibility for own actions looks surprising. 89 % of employees – users of individual DI, identified this feature as an advantage, but as much as 21 % – as a defect. A similar anomaly occurs in the group of users of multi-user DI – a disadvantage, which is the reduction of responsibility for own actions was indicated by 62 % of them, while 11 % indicated it as an advantage.

Therefore, the hypothesis H1 can be considered as only partially proved. Not all employees properly understand the goals of using DI, which may result (Picture 2) in reduction of information security in companies.

Picture 2: Reasons of using DI in enterprises

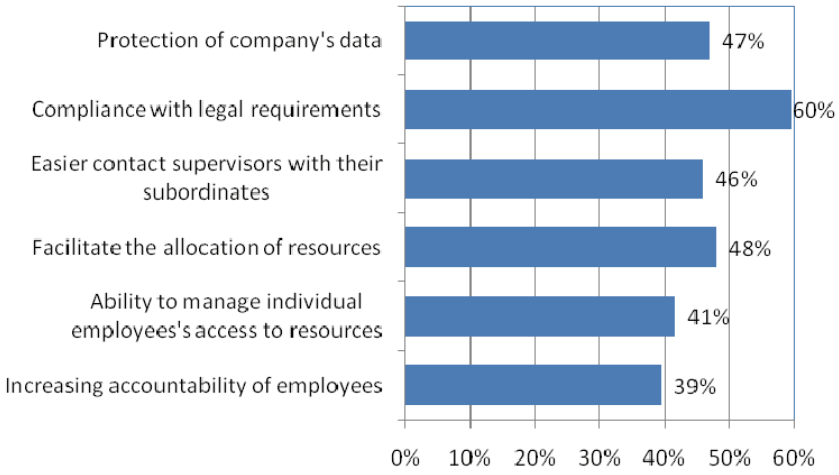


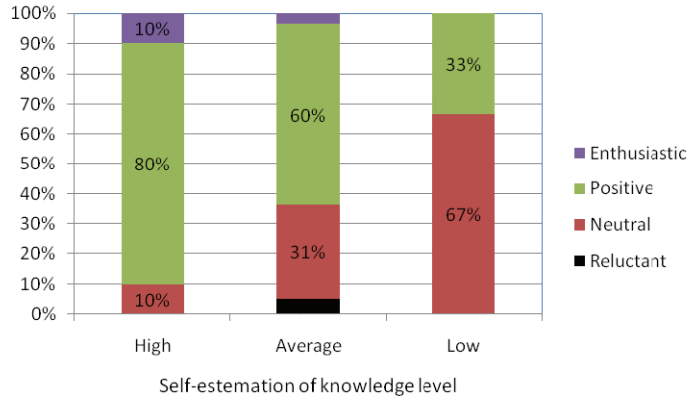
Table 1: Advantages and disadvantages of individual and multi-user DI

Type of DI	Advantages	Disadvantages
Individual	• Responsibility only for own actions (89 %) • Adjustment to user's tasks (78 %) • Easy access to data (21 %)	• Laborious for IT department (49 %) • Laborious for user (41 %) • The risk of incorrect granting permissions (35 %) • Being responsible for own actions (21 %)
Multi-user	• In case of illness an employee can be easier replaced (49 %) • Easy access to company's data (46 %) • One login (no need to log out and log in) (41 %) • Less responsibility - in case of an fault no one bears full responsibility (11 %)	• Less responsibility - in case of a fault no one bears full responsibility (62 %) • Lower data security (62 %) • Granting to extensive privileges (60 %)

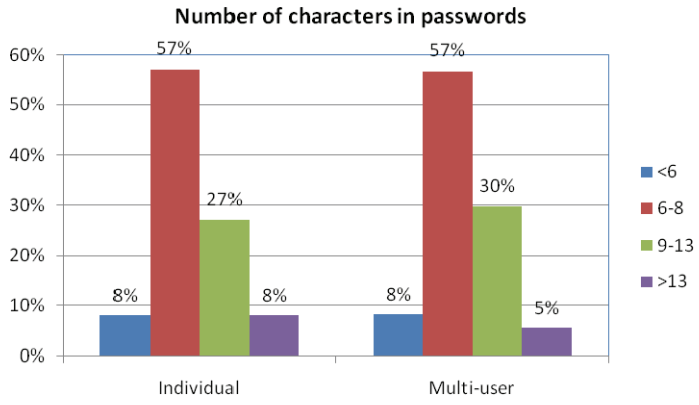
Notice: in brackets there are percentage of respondents indicating a particular option, and each chosen one or two of the most appropriate options

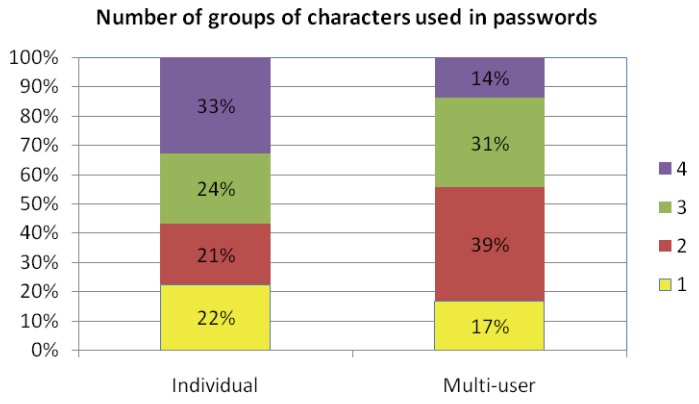
In order to verify the hypothesis H2 the question concerning the acceptability of the need for DI in the company was asked. This question was linked to the question of the self-estimation of own knowledge on the subject. The results are shown in the Picture 3. Positive attitude clearly increases with the level of knowledge about the DI. Unfortunately, in the most numerous group of workers (58 %), i.e. with an average level of knowledge, the ratio of neutral or even lack of acceptance was more than 36 %. Respondents declaring the lack of knowledge were negligibly small group (6 % of all respondents). The hypothesis H2 can also be regarded as only partially verified.

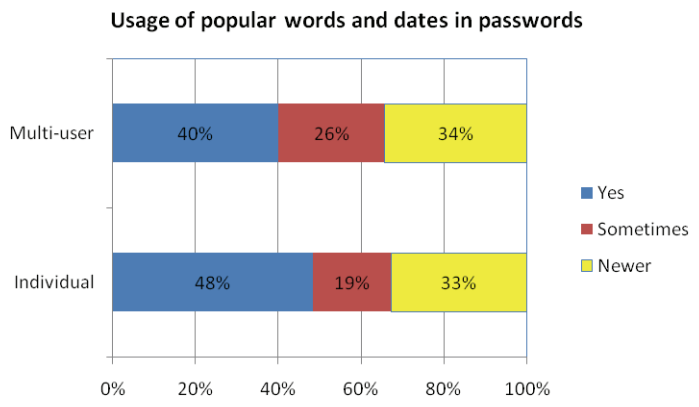
Picture 3: The results of survey on the level of acceptance the need of DI use



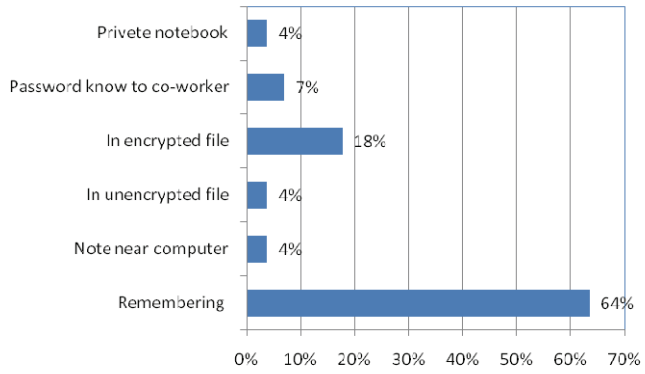
Picture 4: Quality of passwords in multi-user and individual DI







Picture 5: Ways of keeping passwords



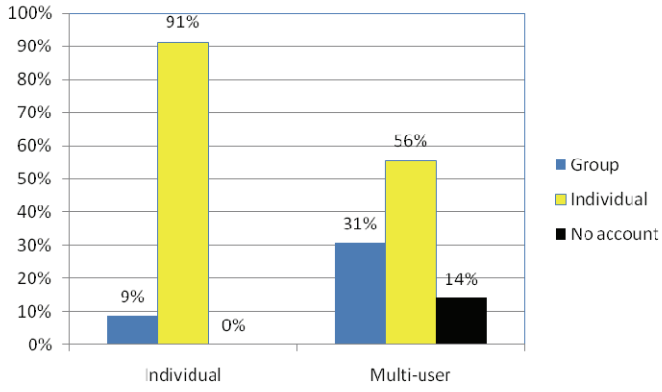
In order to verify the hypothesis H3 there were asked questions about creating and storing passwords, as the basic method of the correctness of application of the security rules concerning DI. Questions focused on:

- the length of passwords,
- types (groups) of characters used in passwords, e.g. lower case and capital letters, numbers, special characters,
- using popular words and dates in passwords,
- ways of storage passwords.

The first three elements constitute the quality (strength) of a password, and therefore its safety. The last one indicates the level of risk of compromising passwords.

Analysis of survey results (Picture 4) indicates that a large group of users (and almost regardless of which group of DI users they come) uses too short passwords and dangerous techniques used to create them. Only about 1/3 of respondents correctly construct the password, i.e. use proper number (more then 8) and differentiation (4 groups) of characters and not use popular words to creating passwords. Analysis of ways of passwords storage (Picture 5) indicates a high level of accuracy of DI using in practice. Dangerous techniques (keeping passwords near PC, in the unencrypted file or on a laptop) are applied by only 4% of respondents. It can be concluded that the hypothesis H3 is only partially true.

Picture 6: The best solution of DI for a company



Analysis of workers' preferences in relation to the types of DI which should be used in the company (Picture 6) indicates the preference to an existing type, indicating the individual DI as more preferred. An interesting result of the research is also the conviction of 14 % of respondents who have the multi-user DI that the company do not need DI at all. Hypothesis H4 has been verified.

6. CONCLUSIONS

Research results clearly show that the questions can be answered only partially affirmatively. In all relevant areas of the impact of human factors associated with ID on the security of information systems, there is quite a large group of employees not understanding the goals of DI application, not accepting the need of using and not realizing it in practice. This group is over 1/3 of all respondents, which allow concluding that the level of IT security is not sufficient. The results practically do not correlate with the type of used DI (multi-user or individual).

The choice of the DI type is often not a decision of user, nevertheless a significant part of users indicates an individual DI as a better solution.

All employees need training. This implicates from the fact that users with wider knowledge on IT security have more positive attitude to the DI. Training will be able to raise awareness and thus the correctness of using of DI in practice (including the strength of passwords used).

REFERENCE LIST

1. Birch, D.G. (2007). *Digital identity management: perspectives on the technological, business and social implications*. Gower Publishing.
2. De Capitani di Vimercati S., & Samarati, P. (2001). Access control: policies, models, and mechanism. In R. Focardi & F. Gorrieri (Eds.), *Foundations of Security Analysis and Design - Tutorial Lectures.* Vol. 2171 of LNCS. Springer-Verlag Press.
3. Feizy, R. (2010). *An Evaluation of Identity in Online Social Networking: Distinguishing Fact from Fiction.* PhD thesis, University of Sussex. Retrieved from http://sro.sussex.ac.uk/6269/1/Feizy,_Roya.pdf.
4. Juszczyk, M. (2011). Impact of Human Factor in Data Security. *Actual Problems of Economics, 6(120),* 359–364.
5. Maler, E., & Reed, D. (2008). The Venn of Identity. Options and Issues in Federated Identity Management. *IEEE Security & Privacy, March/April*.
6. Maliki, T. E., & Seigneur, J. (2007). *A survey of user-centric identity management technologies*. The International Conference on Emerging Security Information, Systems, and Technologies, Secure Ware, 12–17.
7. Miłosz, E., & Juszczyk, M. (2010). Digital Identification in the e-Economy. In A. Zarebska (Ed.), *Using Modern Solutions in Business* (pp. 97–128). Lublin, System-Graf.
8. Miłosz, E., & Miłosz, M. (2011). Digital Identity Management in Polish SMEs. *Actual Problems of Economics, 6(120),* 340–345.
9. Semančík, R. (2005). *Enterprise Digital Identity. Architecture Roadmap. Technical white Papers. nLight.*s.r.o., Bratislava.
10. Shay, R., Komanduri, S., Kelly, P. G., Leon, P. G., Mazurek, M. L., Bauer, L., Christin, N., & Cranor L. F. (2005). *Encountering Stronger Passwords Requirements: User Attitudes and Behaviours.* Symposium on Usable Privacy and Security (SOUPS). July 14–16 2011, Redmond, USA.
11. Windley, Ph. J. (2005). *Digital Identity*. O'Realy.