Marta Juszczyk[1]

DIGITAL IDENTITY ACCEPTANCE AT POLISH LARGE ENTERPRISES: THE SURVEY RESULTS

Digital identity is a way to ensure data security. It is a cheap and comfortable solution, especially when a password is used. However, the data is as protected as password, so employees' behaviour concerning their passwords should be in the area of interests of their supervisors. The acceptance of digital identity is very important. The article presents the results of the survey on digital identity acceptance at large Polish enterprises. Also it discusses the tools for sharpening proper attitude of employees and identifies the gap between their knowledge and behaviour.

Keywords: *digital identity; large enterprises; information security.*

Марта Ющик

ВИЗНАННЯ ЦИФРОВОЇ ІДЕНТИФІКАЦІЇ НА ВЕЛИКИХ ПОЛЬСЬКИХ ПІДПРИЄМСТВАХ: РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

У статті продемонстровано, що цифрова ідентифікація є способом забезпечення безпеки даних. Це рішення є доволі простим та дешевим, особливо у випадках, коли використовується пароль. Однак, дані при цьому захищені настільки ж, наскільки захищено сам пароль. Саме тому всі дії співробітників, пов'язані з паролем, знаходяться у сфері інтересів керівництва. Представлено результати дослідження щодо цифрової ідентифікації на великих польських підприємствах, а також інструменти формування вірного ставлення співробітників до цифрової ідентифікації. Визначено неспівпадіння між знаннями співробітників правил ідентифікації та їхніми реальними діями.

Ключові слова: *цифрова ідентифікація; великі підприємства; захист інформації.*

Рис. 6. Літ. 11.

Марта Ющик

ПРИЗНАНИЕ ЦИФРОВОЙ ИДЕНТИФИКАЦИИ НА КРУПНЫХ ПОЛЬСКИХ ПРЕДПРИЯТИЯХ: РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

В статье показано, что цифровая идентификация является способом обеспечения безопасности данных. Это решение является дешевым и простым, особенно когда используется пароль. Тем не менее, данные защищены настолько, насколько защищён пароль, поэтому все действия сотрудников, связанные с паролем, должны быть в сфере интересов руководства. Представлены результаты исследований по цифровой идентификации на крупных польских предприятиях. Представлены также инструменты формирования правильного отношения сотрудников к цифровой идентификации. Определен разрыв между знанием сотрудниками правил идентификации и их действиями.

Ключевые слова: *цифровая идентификация, крупные предприятия, защита информации.*

Introduction. Implementation of new technology and solutions dedicated to enterprises increase rapidly. To gain or keep competitive advantages new products are implemented (Economist Intelligence Unit, 2007), which have shortened lifecycle. Employees do not always easily follow the changes. It requires efforts to master a manual, but also to learn rules concerning a particular solution. Often, new abilities or skills are needed.

[1] M.Sc., Assistant, Department of Management, Lublin University of Technology, Lublin, Poland.

Large enterprises introduce more solutions in the field of information systems than SMEs. It is due to more funds, more sophisticated needs (e.g., complexity of management) and goals to achieve (larger scale of operation). In Poland, large enterprise is defined as a company which employs more than 250 employees and its annual income exceeds 50 mln. euro or annual balance exceeds 43 mln. euro. There are 3400 large enterprises in Poland (0.2 % of all), they employ 40.6% of total employees (Anam, 2009). So, the problem of adapting employees to growing number of solutions affect nearly half of all employees in Poland. To protect its data an enterprise has to limit the access to data and grant access only to authorized people in a strictly limited scope. To deal with this challenge a digital identity is used.

Digital identity can be defined as "collection of data about a subject that represent attributes, preferences and traits" (Windley, 2005). This set allows mapping real entities into a virtual world. It is also the key element of using information systems, because digital identities enable employees to gain safe access to data stored in information systems of enterprises, and also to communicate via Internet (Milosz and Milosz, 2011).

Other basic definition of digital identity treats it as "set of claims made by one digital subject about itself or another digital subject". To gain access a user must prove a claim. It can be performed using employee's knowledge (e.g., password), special equipment (e.g., token) or some unique, personal features of, a user (e.g., retina). Each of these methods of authentication has benefits and drawbacks.

Problem definition and literature analysis. Passwords, due to low cost and easiness of use are the most common solution of granting access (Semancik, 2005). But even this easy method of authentication has some problems to deal with (Gutierrez and Feigenbaum, 2006). To secure a digital identity a password should be safe, which means, for example, proper length, different char used, avoiding meaningful phrases or regular changes of password, and also keeping it in secret (Semancik, 2005).

Rules concerning passwords are well known, but not respected. It can be confirmed by analysis of disclosed passwords for emails e.g., Hotmail (Maj, 2009). Passwords were easy-to-guess (e.g., 123456), contained names plus number (e.g., Nicole1) or simple word (e.g. monkey). These passwords were for private usage, but what type of password does an employee choose? Probably, if there are no guidelines, an employee chooses a password similar to the one used in private life.

So, why employees do not pay attention to acting in accordance with instructions? Maybe there is no instruction? Or maybe employees do not accept the solution? Acceptance is connected with attitude, which includes actions taken by employees.

The importance of technology acceptance is even greater in situations when there is no possibility of full control of taken action (e.g. using one account for a group of employees). Then acceptance of a particular solution by an employee can be one of elements of heavy influence on solution performance.

Problem formulisation. Large companies are very important for Polish economy. Due to their size, access to data is more complicated (divisions, level of access etc.) and more difficult to control. The most preferable situation is when employees behave in a safe way without additional incentives. Partly this state can be achieved by convincing, not forcing. And there is a question: what should be stimulated and how to increase the acceptation and to form proper attitude to digital identity? Moreover, there are researches (Pastuszak, 2009) reporting insufficient organizational skills in the area of e-business of Polish managers; lack of investments in security of Polish companies (Webhosting.pl, 2011); others (Shay et al., 2005; ACMA, 2009) indicate lack of correct behaviour concerning passwords among employees. So, what is the current situation in area of managing the acceptance of digital identity and how to improve it?

Research methodology. To find factors influencing the acceptance of digital identities, the research based on interviews and questionnaires was conducted. To avoid excessive number of questions or misunderstanding, digital identity was defined as a computer account identified by a login and protected by a password. The questionnaire covered different areas as a part of larger research (supported by EU).

The main aim of the study is to diagnose the current acceptation of digital identity and to present important factors on managing acceptation.

In the preliminary research (interviews with top management) two important factors influencing employees are identified as trainings and proper motivation.

The impact of these factors on employees is the attitude to digital identity represented by:

- emotional component;
- behavioural component;
- cognitive component.

At the beginning of the research hypotheses are defined as:

H1. Using login and password is generally accepted.

H2. The fact of the acceptance affects all the components of attitude to digital identity equally.

H3. Training affects the attitude to digital identity.

H4. There are simple actions which can improve employees' behaviour concerning using digital identity.

Research results. Respondents at large enterprises fulfilled the questionnaires. All incomplete or incorrect forms were rejected, as well as the forms fulfilled by employees who do not use computer accounts at work. This reduced the number of the test sample to 25 employees of different large enterprises operating in different fields (healthcare, education, IT, insurance, trade, production, telecommunications, finance, real estate, distribution, shipping, banking, administration, marketing research etc.).

The questionnaire was fulfilled by 10 women and 15 men. The youngest respondent was 21, the oldest – 57, average age was 32.5.

All the respondents have experience with using digital identity protected by a password, 64% used tokens and 8% – fingerprint reader. Reported actions related to using accounts are: logging in and out many times a day (92%), forgetting password (52%), recovering password (40%), entering wrong password (36%) and password rejection or system error (32%). Despite this fact, all the participants of the research perceive using computer account as easy. However, 32% of the respondents admit that it is time consuming.

The level of acceptation of digital identity is high (H1). All the respondents declared this solution is necessary in their company (Fig. 1), and only 12% chose less safe multi-user accounts.

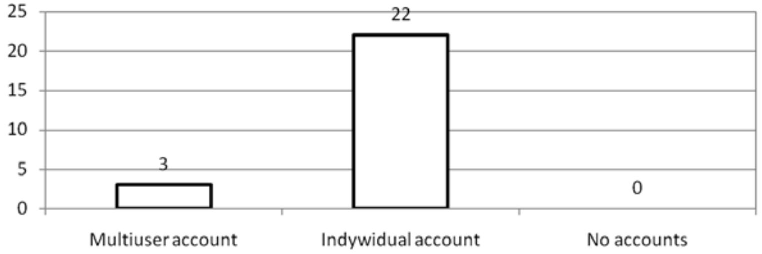

Figure 1. **Answering to the question on the cognitive component: In your opinion, what solution is the best for your company?**

Most users have positive attitude to digital identity (Fig. 2). Only one person has negative attitude to this solution.

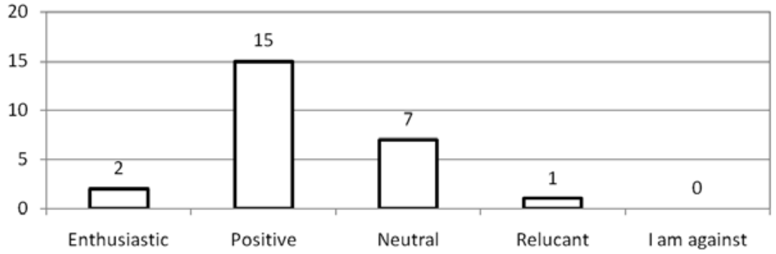

Figure 2. **Answering to the question examining the emotional component: What is your attitude to digital identity?**

Despite conviction of the need to use digital identity (cognitive component) and positive emotional attitude, only 28% of employees declare they follow the rules (Fig. 3). At the same time only in one company there is no security policy, and 4 persons are not sure if their companies have security policy or not. It is a gap which should be managed to avoid data leak or other consequences of carelessness. This partially confirms H2, but it means there is no simple relationship between acceptation and actions taken by employees.

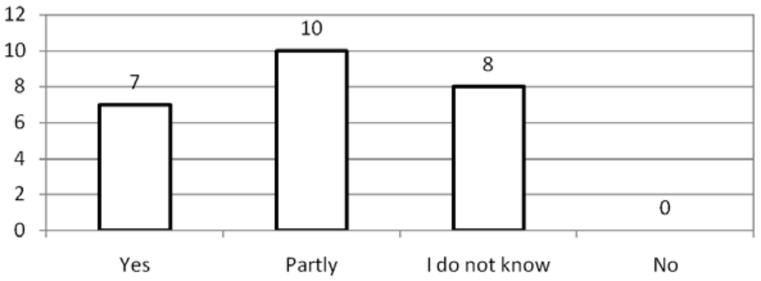

Figure 3. **Answering to the question examining the behavioural component: Do you follow the rules concerning using computer accounts?**

It has been assumed that the gap between knowledge and behaviour can be diminished by two previously mentioned factors: trainings and proper motivation.

The impact of training on attitude is undoubted (Fig. 4). Trained employees are more confident of their knowledge (52% of the respondents perceive their level of knowledge as high), have more positive attitude (82% – positive or enthusiastic), and almost half of them declare that everyone in the company follows the rules (42.5%). On the other hand only one employee without training declares high level of knowledge, positive attitude is declared by 50% of the respondents, and noone declares that rules are obeyed. This confirms H3.

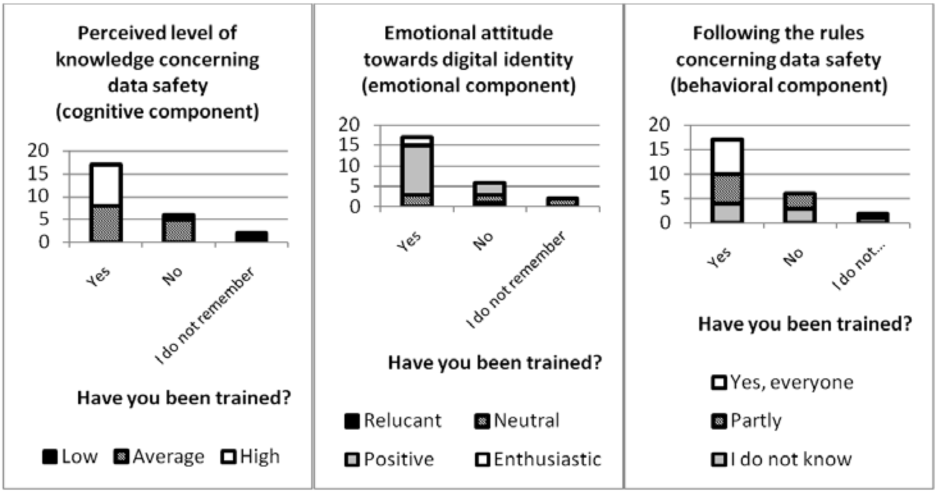

Figure 4. **Impact of training on knowledge, perception of digital identity and behavior of employees**

The Respondents were asked to indicate up to two the easiest to accept (Fig. 5) and the most effective (Fig. 6) motivating factors.

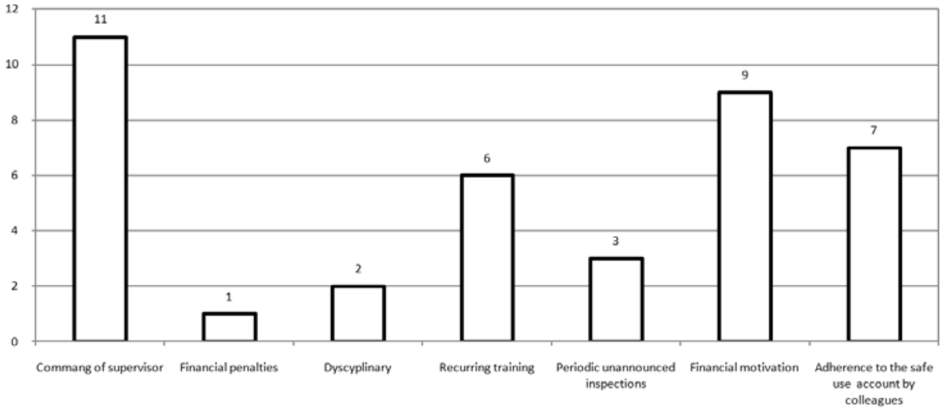

Figure 5. **The easiest to accept motivator of safe use of computer accounts**

For them, the easiest to accept is the direct command of a supervisor (11 answers). The second place in ranking is occupied by financial motivators — bonuses to salary taken away in cases of security breach (9 answers). The third way of motivating safe use of accounts is good example of coworkers (7 answers).

The respondents were asked about the most effective ways of motivation (Figure 6): good example of coworkers (11 answers); training (10 answers) and bonuses and command of a supervisor (8 for each).

This confirms H4 and indicates the direction for effective motivation.

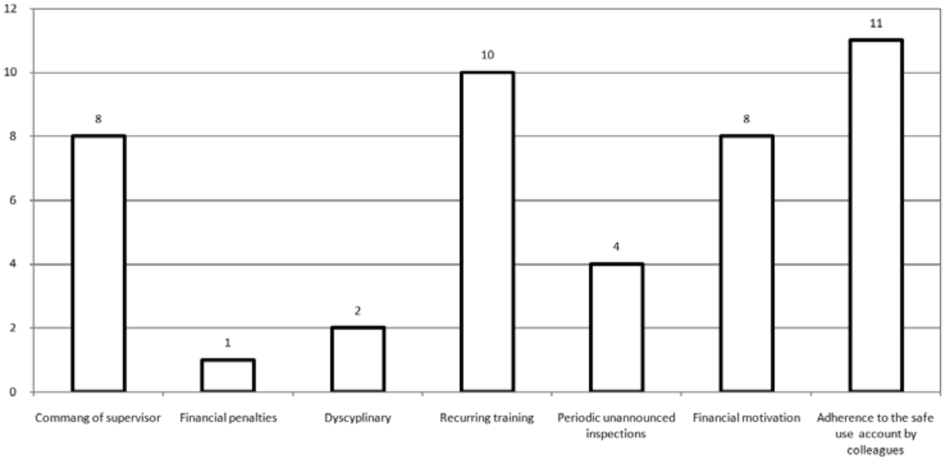

Figure 6. **The most effective motivator of safe use of computer accounts**

Conclusions. Data security is a matter of great importance. Digital identity is a way to obtain needed protection for data. Human factor is often the weakest link in security. Managers should develop proper attitude of their subordinates. Firstly, they should establish rules concerning using computer accounts, equip employees with proper knowledge, strengthen the positive perception of digital identities and promote appropriate behaviour. Many of these actions are costless, depending only on a manager's is will.

Employees at large enterprises have positive attitude to digital identities. They accept the solution, but have problems in safe using of accounts. It can be the effect of lack of control and a dose of discretion of employees in this matter. This means that large enterprises have to solve the problem of the identified gap.

References:

ACMA (2009). Attitudes towards use of personal information online. Quantitative research report.

Anam R. (2009). The economic situation of large companies. http://www.egospodarka.pl/39515, Sytuacja-ekonomiczna-duzych-firm-2009,1,39,1.htm,l [2011, Dec 12]. (in Polish)

Economist Intelligence Unit Report (2007). Digital identity authentication in e-commerce.

Gutierrez A. J., Feigenbaum J. (2006). Towards Better Digital Identity Management, Sensitive Information in a Wired World. http://zoo.cs.yale.edu/classes/cs457/spr06 /info_paper.pdf, [2011, Dec 12].

Maj M. (2009). 123456 – najpopularniejsze haslo w Hotmail. Dziennik Internautow Bezpieczenstwo, 8th of October 2009. http://di.com.pl/news/29003,0,123456_-_najpopularniejsze_haslo_w_Hotmail.html.

Milosz E., Milosz M. (2011). Digital identity management in Polish SMEs. Actual Problems of Economics, No. 6, pp. 340-345.

Pastuszak Z. (2009). Theory, practice and strategic challenges of the future company. Przedsiebiorstwo przyszlosci, No. 1, pp. 10-28. (in Polish)

Semancik R. (2005). Enterprise Digital Identity. Architecture Roadmap. Technical white Papers. nLight. s.r.o., Bratislava.

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.

Webhosting.pl report (2011). IT Security in Polish companies. (in Polish)

Windley Ph. J. (2005). Digital Identity. O'Reilly Media, Inc.

Стаття надійшла до редакції 17.01.2012.