POLISH JOURNAL OF MANAGEMENT STUDIES
Otti Cs., Kolnhofer-Derecskei A.

2018
Vol.17 No.2

INTRODUCTION TO THE BIOMETRIC ACCESS CONTROL SYSTEMS FOR MANAGERS: WHICH ERROR INDICATOR MATTERS IN THE SELECTION?

Otti Cs., Kolnhofer-Derecskei A.[*]

Abstract: The managers in the business sector have to face security management issues on a daily basis and the present article analyses and discusses one of its segments, namely the biometric systems. The decision-maker is presented with a number of professional data before the implementation of such a system, although the opinion of the final user will be determinant regarding the use of the system. Following the dual engineer-manager approach, the present study first introduces the biometric systems through the engineering metrics and concepts because the decision-maker learns the errors of the system through these indices. The research also highlights the fact, that the final user is far less sensitive. However, it is a principal factor in all the security investments whether the users are able and willing to use the system properly. It is even more so in case of biometric access control systems because the algorithms operate with probabilities and the users can never be sure that they are recognized with 100% accuracy. The error values provided by the manufacturers of biometric systems are not available and because these are algorithmic data, the difference can be of several orders of magnitudes between the actually measured results. The article publishes the results of a quantitative research and determines the users' individual subjective acceptance threshold regarding the errors of access control systems. On the basis of this, the biometric systems could be evaluated from the users' point of view as well.

Key words: FRR, biometrics, user acceptance

DOI: 10.17512/pjms.2018.17.2.17

Article's history:
Received February 15, 2018; *Revised* May 7, 2018; *Accepted* May 26, 2018

Introduction

The relevance of the examined topic could be supported by the recent implementation of GDPR; however, we do not discuss the legislation of data handling because our research focuses on another segment of security management, namely the biometric access control systems. The selection and introduction of such a system belongs to the competence of senior executive management. These managers, however, mostly get the information based on the error indicators tested by engineers. The aim of the present article is to review the basic concepts in order to get a better understanding of this area. It should also be

[*]**Csaba Otti, MSc.**, Óbuda University, DonátBánki Faculty of Mechanical and Safety Engineering; **Anita Kolnhofer-Derecskei, PhD,** assistant professor at Óbuda University, Keleti Faculty of Business and Management
✉ Corresponding author: otti.csaba@bgk.uni-obuda.hu
✉derecskei.anita@kgk.uni-obuda.hu

highlighted that the users are much more receptive; the error indicator they perceive is different by orders of magnitude from the technical error values of the system. First, however, it is briefly explained why it is important to deal with this topic in the field of management. As it is discussed by Peltier in his book: "an overall security program helps the enterprise meet its business objectives or mission by protecting its physical or financial resources". (Peltier, 2016)In order to achieve this, it is inevitable that the decision-makers (security personnel) are well trained and knowledgeable in technical sciences, too. It should be added - as Sennewald and Baillie also underlines - that "the security division is accountable for the employees" (Sennewald and Baillie, 2015).

These days there are an increasing number of articles and research dealing with the issues of security management (Kliestik et al., 2018, Belás et al., 2017; Kuril, 2018; Limba and Šidlauskas, 2018). Soomro et al provide an excellent summary of the professional literature sources. Their study highlights the interdisciplinary cooperation of engineering and management sciences (Soomro et al., 2016). One of the main areas of security management – besides IT security - is the physical security; the main elements of which are: the mechanical protection, electronic protection and manned protection. One of the basic tasks of providing security is to ensure that only the authorised staff can have access to the given facilities, persons or information (Oláh et al., 2017, Oláh et al., 2018). The major part of security systems is focusing on this task. There are three types of basic technologies in the field of automatic identification (access control systems): knowledge based (PIN code, password); asset-based (card, phone) or biometric identification (a physical characteristic). (Otti, 2016; Piotrowska et al., 2017)The automated, electronic biometric identification has gone through an enormous development in the last fifty years. The law enforcement authorities have an increasing demand to be able to identify people quickly and credibly, practically anywhere. Parallel with this, it is more and more necessary in all the areas of life to identify users and entrants and to authenticate their access. On the other hand it is fairly obvious that the users' acceptance towards these technologies or devices has a key role in the success of implementation and everyday usability. (Dillon and Morris, 1996)

In the research first of all those civil biometric applications were identified where the biometric identification was crucial in terms of operation: these are the staff entry and attendance recording systems in companies with high number of employees. (Otti, 2016) It is regarded crucial because - due to the high number of staff - the system should be quick and should have a low false rejection rate (FRR) value. The majority of almost 100 biometric systems, that have been implemented in Hungary in the last 20 years and examined in our research, failed. Even in our days the success depends only on „sheer luck". Having analysed this phenomenon we started to test biometric devices in ABI (Applied Biometrics Institute) in 2010. By examining any device of any supplier it was revealed that the FRR data provided by the supplier were different from the actual values by several orders of magnitude. The primary reason for this was that the suppliers provide the results of

algorithmic or – in other words – technological tests and they do not calculate with users, implementation or environmental conditions. The next question that came to us was: how could there exist any successful biometric system at all? Or approaching it from another angle: can it be decided about a biometric device during the tender whether it is going to function properly or not?
Therefore we turned to the users and asked them how they perceived this issue. The hypothesis was that the people would accept higher False Rejection Rate even by 2-3 orders of magnitude as serviceable. In the expert and focus group examinations carried out in the previous phases of research (Otti, 2017). We elaborated the set of questions, which the quantitative research was based on. The present study analyses the questions and summarises the results on the basis of 653 responses.

Literature: Characteristics of Biometric Systems

Hereinafter the technical parameters of biometric access control systems are summarised in a nutshell. On the basis of the related ISO standard (ISO/IEC, 2006) andShimon's article Biometrics in Identity Management: Concepts to Applications (Shimon, 2011)the biometric devices are basically sample recognising systems and in general they consist of subsystems as it can be seen in Figure 1.

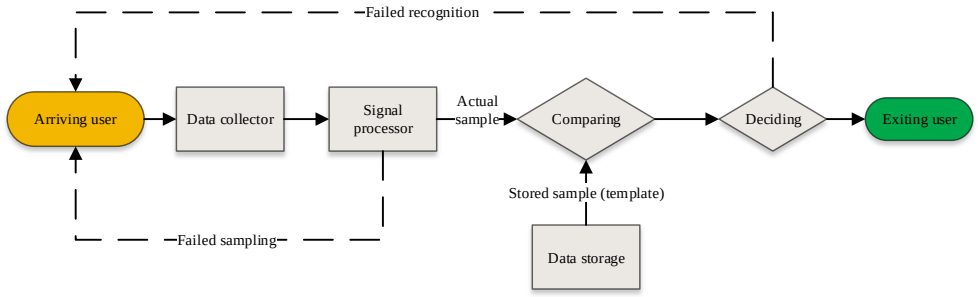

Figure 1. Subsystems of a general biometric device

The data collecting subsystem is responsible for taking the biometric sample of the user. The errors entered into the system at this point would run through the whole identification process. The task of the sign processing subsystem is to extract those features from the samples, which make them unique. The data storage stores the collected and coded biometric data for later comparison. These data are also called templates in biometrics. The storage can be central (on one computer or server) or local (e.g. on a smart card or individual media device). The Regulation (EU) 2016/679 practically bans the central storage of biometric data from users. The comparing subsystem compares two samples and creates a similarity score. This score indicates the certainty that the stored template and the sample taken are from one and the same person. The biometric identification systems are always probability-based; therefore 100% match would never exist. As opposed to this, in

case for example a cryptographic or password-based system the successful identification always requires 100% match. Since the meeting of a person and a sensor can never be exactly the same twice, therefore the system generates a similarity score instead of a simple „yes" or „no" response. The decision-making subsystem compares the generated similarity score to a preliminary determined limit in order to decide about the success or failure of identification. But sometimes there are errors. The control and identification errors can be traced back either to matching (false match or false non-match) or sampling errors (sampling failed, entering into system failed). When these basic errors lead to a decision-making error, it can be due to several different factors, for example the number of comparisons required; decision-making policy or simply whether the identification was positive or negative. (Jain et al., 2004; Androniceanu, 2017a)

A biometric identification system can generate two types of errors (1) It can produce false match of biometric samples from two different persons and identify them as match (False Match: the index in references is FMR - False Match Rate or FAR - False Acceptance Rate) (2) Two measurements from the same person are identified as belonging to two different persons (False Non-match: the index in references is FNMR – False Non Match Rate or FRR – False Rejection Rate).

There is a trade-off curve in every system between the false match rate (FMR) and the false non-match rate (FNMR). If the system is configured in a way that it is less sensitive to confusing factors and has better acceptance of the users' samples, the FMR will be increasing; if more secure settings are created, then the FNMR will be higher (Androniceanu, 2017b). ROC (Receiver Operating Characteristics) and DET (Detection Error Trade-off) curves are generally used to describe the performance of biometric systems ((Springer, 2013; Horváth and Kovács, 2013).

The references do not offer any (or they offer more) commonly used and accepted definitions of indices characterizing biometric systems. Mostly the ISO/IEC 19795 standards of 2006 and 2012 are applied. (ISO/IEC, 2006; ISO/IEC, 2012) Here we do not detail all of them only we focus FRR because that has important significance in practice. The False Rejection Rate is seemingly a secondary index in the field of biometric identification. This may be the case because FAR (False Acceptance Rate) is far more „terrifying" in terms of security, as it means that non-authorised persons (impostors) may enter the protected area. It is true in many applications, but in the area of physical security, in case of mass occupancy establishments (entry and attendance register; more than 300 employees) there has not been any application in Hungary in the last 20 years where this factor dominated. It is easy to prove if mathematical risk analysis methods are used;as well as the time and success of entering the users is an important aspect in the implementation (Michelberger and Horváth, 2017).

On the basis of the professional literature sources we have processed, estimating, measuring and providing FRR was almost always limited to technological results – which is not surprising as this is the only test type, which can be controlled well, can be run on a large mass sample and is able to set up a clear order among the

algorithms. The manufacturers would indicate these FRR values on the specification of their devices, usually in the 0.00001% - 0,01% range.(Hanka and Werner, 2015)
Examining the results of scenario tests and tests under live conditions, it has been concluded that in reality the users meet false rejection in the 1%-70% range. It means that the difference can be at least 2 or even 6 (!) orders of magnitude between the promise in the specifications and the actual results. Since the values in the specifications cannot be measured in the practice, this leads to two outcomes in the decision-making regarding a security investment: (1) The devices of all the manufacturers meet the requirements. (2) It cannot be decided which system is more suitable for the given task. Therefore the decision points are shifted and other aspects - for example the price –are given priority.

Scenario FRR Tests (Research 1)

On the basis of the related ISO standards regarding the testing of biometric systems as well as own methodological developments, the same conditions were created for the scenario tests as those with which the users meet in real life. Such as for example the dependence on light conditions in case of a face recognition device, with the testing of which it can be exactly determined how a device installed outdoor would behave under the sunlight at different times of the day. (ISO/IEC, 2012)As it has been expected, the FRR values deteriorate when the circumstances are deviating from the ideal. The difference between devices and the decision about usability of each device depends on how quickly and to what extent the results are deteriorating. (Kovács et al., 2012)
Procedures that are as close to real conditions as possible have been elaborated enabling the accurate documentation of conditions and circumstances of tests in order to ensure reproducibility: (1) Positioning sensitivity: the perfectly positioned sample is rotated and shifted and the changes in FRR are measured. (2) Measuring throughput in relation to enrolled users and samples. (3) Contamination of the sample: for example a wet finger. (4) Distortion of the sample: for example a wounded finger or a ring. (5) Effects of environmental changes: lighting, temperature, and humidity. (Stan and Li, 2015)
Hanka's publication (2013) gives an excellent summary for the analysis of statistical backgrounds of FRR measurements. In this work Hanka confirms and expands Doddington's rule of 30 on biometric fingerprint identifying systems. The rule says that to be 90% confident that the p probability is within ± 30% of the relative frequency calculated on the basis of experiences, there must be at least 30 errors. In the current case the p probability is the FRR value and – according to the principle - 30 errors should be measured in order to accept the given FRR level. It means that 300,000 events or tests should be made for the FRR=0.01% measurement of an average biometric device. This is virtually impossible to carry out. Yet we got interpretable results in the reality; the best example for this is the FRR dependence of a fingerprint identifying equipment on the number of enrolled

samples. According to the measurement methodology, the nominal user capacity (500 people) was filled up with 50-person increments and 300 measurements were made in every measurement points. The results can be seen in the following figure.

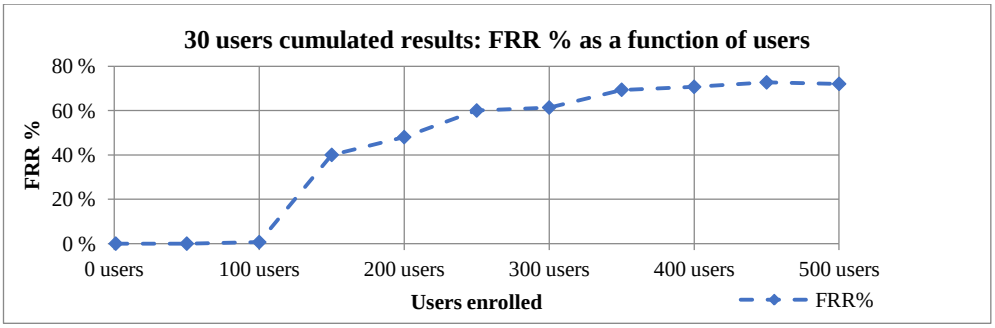

Figure 2. Results of face recognition scenario test. FRR% as a function of enrolled users

The implementation of such a device is a rather costly investment. Nazareth and Choi also examined this; using a system dynamics model, their study evaluates alternative security management strategies through an investment and security cost lens, to provide managers guidance for security decisions. (Nazareth and Choi, 2015)When ranking the systems, the technical specifications of the system as well as other aspects should also be considered. Regarding the success of implementation and use, the opinion of the final users is very important. They may perceive the false rejection as "the door is stuck". How do they interpret this and with what error values would they still feel the system acceptable? These questions are discussed in the next chapter.

Users' Acceptance (Research 2)

The subject of research in this chapter is the final user, who is tested with the methods of social science, through their introspective responses given to hypothetical, imaginary situations. The objective of the current research is to survey when and to what extent the people regard a biometric access control system usable in relation to the number of their failed entries. Previous study (Otti, 2016) helped to define the spontaneous responses, experiences and feelings of people. Due to this, the biometrics relates was taken out from the definition, then the access control system, too. Then it was simplified to a stage that the question was about passing through a door, which is sometimes stuck and cannot be opened. In this example the number of failed entries can be interpreted in an analogous way but it is not trivial, which value it corresponds with. Finally, the FRR value is chosen because it contains the algorithmic FMR and FTA (Failure To Acquire) values but it does not include the FTE Failure to Enrol rate, which cannot be modelled. The question was as follows: *„Imagine that you have to go through a*

door in your workplace/school 5 days a week, four times a day. This door usually works well, but ……. (frequency of door jam) times it is stuck and you have to try again to open it. To what extent do you regard the door usable?"

The hypotheses drafted in our research are as follows:

H1: There is a correlation between the frequency of being rejected and the presumed usability of the system.

H2: The acceptance threshold of people is higher by several orders of magnitude than the FRR False Rejection Rate provided by the manufacturer for the device.

If the hypotheses can be confirmed then – on the one hand - the values based on the scenario tests can be validated statistically; on the other hand the usability of the system can be actually predicted in the given application.

The frequency of door jams is determined as a function of the number of entries and the following units were used (1) once a day (the most frequent) (2) once a week (3) once a month (4) once a year.If we presume that the respondent goes through the gate in question every weekday at least four times (2 entries and 2 exits), then calculating with 20 workdays per month on average it means 960 passes per year, therefore the relative frequency of being stuck per year is as follows (1) 25% in case of one jam per day (2) 5.415% in case of one jam per week (3) 1.25% in case of one jam per month (3) 0.104% in case of one jam per year.The presumed usability was measured on a four-stage semantic differential scale using the following stages: (1) unusable (2) less usable (3) usable (4) perfectly usable. Both criteria mean data measured on ordinal scale. The following statistical methods were used in the analysis: descriptive statistics; interval estimation (with 90% confidence interval, which was justified by Doddington's rule that is used for the evaluation of biometric systems); cross table analysis (with α=0,05 significance test); non-parametric hypothesis tests (again p = 0,95), and regression analysis.

Methodology

The data were collected in March and April 2017 among the students of the Óbuda University (446 persons, 60.8% of the respondents) and the members of MENSA Hungar IQ (197 persons, 26.8% of the respondents), as well as students from other universities (91 persons, 12.4% of the respondents). Our choice of target group is justified by two reasons: on the one hand the students on the campuses of the Óbuda University already meet and use access control gates on a daily basis, and, on the other hand, they will form an organic part of the labour market, where – according to our experiences – the majority of enterprises and all the large-scale companies use similar access control systems. Out of the students of Óbuda University, 390 persons are studying at the Donát Bánki Faculty of Mechanical and Safety Engineering; they not only meet such systems but also study about them. Some of the respondents (497 persons) are already employed, typically in areas where they encounter such systems. A questionnaire was used in the research, the content of which was partly based on former research (Otti, 2016), partly on review of professional literature sources. Since the respondents had to assess the issue of

being rejected at the door not in a real but in an imaginary, hypothetical situation, the questionnaire was tested several times. Following the data cleansing, responses from n=734 respondents were processed. This number of elements was further reduced to 653, which covered those respondents who answered all the questions. The distribution of respondents was the following: By gender 74.4% (486 persons) were male and 25.6% (167 persons) were female; it is due to the profile of Óbuda University.
As the sampling was not based on random selection and our aim was to increase the number of sample elements, therefore our sample has high element number but cannot be regarded as representative from all aspects.

Results

There is a significant correlation (sig. $p < 0.05$) between the frequency of being rejected and evaluation of usability. The lower is the frequency of rejections, the higher is the satisfaction. The quantifiable value of correlation by Pearson correlation is $R = 0.543$, which is a moderately strong correlation.

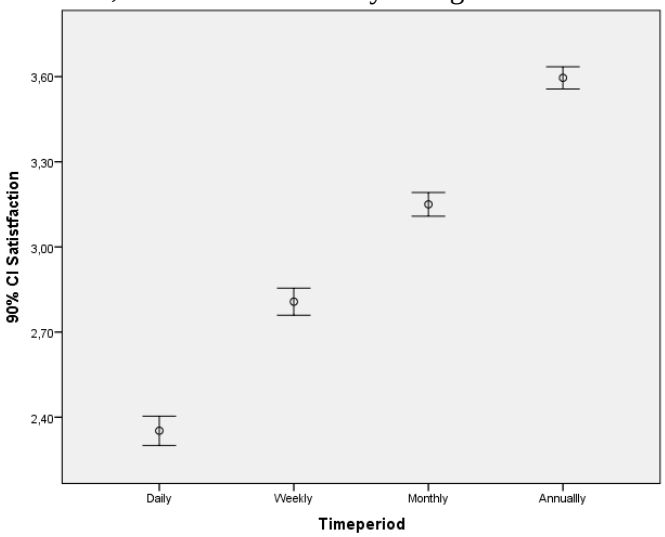

Figure 3. Averagesatisfaction of respondents as a function of the frequency of rejections, with 90% confidence interval

If the time unit is examined not on an ordinal but on a ratio scale, that is the frequency of rejections is examined in the above described percentage (relative) distribution, the value will be very similar ($R = - 0.479$, the negative value is justified by the fact that the lower is the frequency of being held up, the higher is the user's satisfaction). This moderately strong significance of the correlation enables to fit a regression function on the data. During the fitting, the frequency of rejections was examined in the percentage of time unit. The best fit could be observed in case of the logarithmic function, which is demonstrated on Figure 4

below. The value of constant is 2.1054, which means that there is a neutral reaction to the stuck door, which decreases the value of the usability of the device by increasing the frequency of rejections. In this case, one per cent growth in the frequency of being stuck (1% of four-a-day passes, 960 times a year) will lead to decline in the users' usability sense by 0.224 unit (considering on the above described 4-stage scale). We should realise a strong similarity between Figure 2 and Figure 4 that failures curves are similar but the acceptance levels differ.

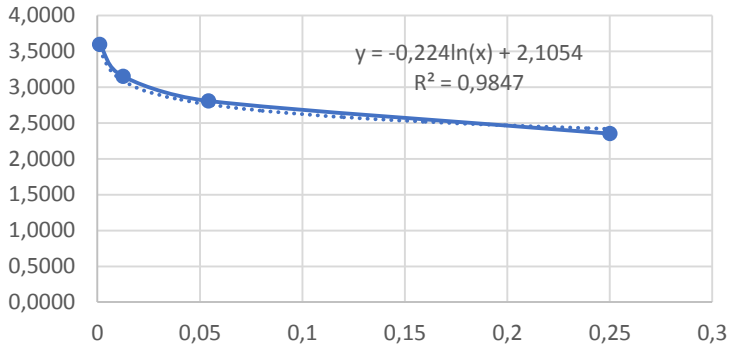

Figure 4. Regression function fit on the general satisfaction level of the respondent as function of the frequency of rejections (X axis: relative frequency of rejections per year, Y axis: degree of usability/satisfaction level)

The examination has confirmed the H1 hypothesis, which assumed that there is a correlation between the frequency of rejections and the presumed usability of the system. Moreover, this correlation is strong enough to fit a logarithmic regression function on it. It should be repeated, however, that the explanation power (Rsquared) is 0.295, which means that the frequency of rejections explains the satisfaction of the user only to an extent of about 30%. Therefore the question arises, what else can affect the user's satisfaction. During the survey, in addition to the demographic characteristics, the users were also asked about their workplace satisfaction. The reason for this was that the respondents were deliberately not given the questions in sequential order; therefore the questions put between responses decreased the saturation and maintained the interest of the respondent. (1) How do you feel now? (2) How satisfied are you with the information received for your work/studies? (3) How much would you recommend your current workplace/school to others?

Again the answers could be given to this on a semantic differential scale. Although it could be interesting, but the present article does not cover the one-by-one analysis of responses given to these questions; only those overlaps are discussed, where the user's actual general mood and their feelings towards their work had an impact on the usability value we examined. The general device satisfaction level was examined in the comparison; and the significant correlations (sig. $p < 0,05$)

that were found had the following features: (1) those who felt better and marked a higher value on this scale, evaluated the device as more usable in general (Cramer value 0.179); (2) the more the respondent felt that they receive substantial information, the more satisfied they were with the device (Cramer value 0.179); (3) in this case the direction of the relation (cause and effect relation) was not identified but there was a significant correlation between the device satisfaction and the degree of recommendation (Cramer value 0.161). The strongest correlation was in case of information; in another question, the ratio of predictability was indicated as the main source of stress in the workplace. This indicates that education and appropriate information flow may reduce uncertainty and by thisimprove the feelings towards and acceptance of the device. It is obvious that the correlation is everywhere significant but very weak, therefore the explanatory power of the above model would only be weakened by these factors in case of applying a multifactor regression model, therefore we accept the two-factor model.
According to hypothesis H2, the acceptance threshold of users is higher by several orders of magnitude than the false rejection rate (FRR = 0,01%), which is usually provided on the datasheets. There is an approximately 3% FRR belonging to the 3.00 „Usable" value on Figure 4. Therefore hypothesis H2 has been confirmed, too.
Cavusoglu et al got similar outcomes from testing the security awareness of organizational users. They regarded the appropriate training in the early phase and later the prudent control as the most important elements in the implementation of such a system. (Cavusoglu et al., 2015)

Summary and Conclusions

Peltier (2016) systematizes those features, which should be considered before the implementation of security-assisting systems. (Peltier, 2016) Focusing on the users, the present research compared the acceptance rate (usability index) given by them and the technical parameters of the system. Both the technological and organisational aspects are critically important, but both of these are closely related to people. As our research has also concluded, the individual users are less sensitive than the certified FRR. As the sense of security is decreasing, more and more security and biometric systems are implemented all over the world. The acceptance by the users is closely related to their ability to use the system.
Two hypotheses were tested in the present article:
H1: There is a correlation between the frequency of being rejected and the presumed usability of the system. ACCEPTED
The system may reject the final user during the access control for several reasons. The final user, however, would not perceive the FRR value at all, for them the door is stuck and they cannot enter. They cannot achieve their objective; therefore they will not be satisfied with the system. Nevertheless, this rejection rate will still be lower even with a much more frequent failure to enter than what could be regarded acceptable on the basis of the technical parameters.

H2: The acceptance threshold of people is higher by several orders of magnitude than the FRR False Rejection Rate provided by the manufacturers for the device. ACCEPTED

Both hypotheses have been confirmed and thus it has been proved that the actual FRR values measured in scenario tests can be evaluated in this range. Under given security conditions it should be determined what value of user acceptance would be suitable for business decision-makers and the biometric access control systems should be calibrated to this value.

Discussion

Managers have a great responsibility in choosing, implementing and ensuring the successful use of the appropriate device. In the selection phase, besides knowing the technical parameters, the satisfaction of final users with the device can be achieved with further support. It has also been revealed that education and information flow can significantly improve acceptance, which base on a properly designed knowledge transfer system. 'However, a properly designed transfer system is a prerequisite for effective knowledge transfer in an intra-organizational network, which can assist in the generation of competitive advantage.' (Sroka et al., 2014)On the other hand, the security management approach is an innovation approach, similar to the social innovation approach, which says that the enterprise engagement in that kind of activities "may provide the background conditions for the creation of additional profit opportunities while generating social value; the possibility of obtaining tax benefits from government; and the receipt of benefits from the public and private sectors (mainly by involving the additional investment capital)."(Shpak et al., 2017)

The acceptance of the technology by the users can be clearly observed in the course of implementing an ERP or HRIS system. By quantifying that the people still typically accept an approximately 3-5% inconvenience; this value presumably can be applied in the implementation of management support systems and software and in case of organisational development projects, too. Our results can also be used in employee journey mapping analyses. It means that without training and improving the commitment to the given system this degree of inconvenience is still accepted by the employees without any significant decline of satisfaction.

At a fundamental level, our study provides managers with clear findings regarding acceptance of security and helps to decide about that kind of investment. This article also advises managers to adopt a more holistic approach to information security management to include: management participation from top-level management and the involvement of strategic decision makers to the thorough understanding of the technical parameters of devices. However, the motivations of users, their human nature; in other words, the soft factors in addition to the hard, technical factors will also have an important role. This has been highlighted by Safa and Von Solms, too: "now we can say that information security knowledge sharing, information security collaboration, and complying with information

security organizational policies and procedures are organizational aspects of information security that should be taken into the consideration by both academics and practitioners." (Safa and Von Solms, 2016)

Acknowledgements

 *Supported By the ÚNKP-17-4/I. New National Excellence Program of the Ministry of Human Capacities*

References

Androniceanu A. 2017a, *The three-dimensional approach of Total Quality Management, an essential strategic option for business excellence*, "Amfiteatru Economic", 19(44).

Androniceanu A. 2017b, *Hospital management based on the relationship between doctors and patients*, "Administratiesi Management Public", (29).

Belás J., Mišanková M., Schönfeld J., Gavurová B., 2017, *Credit risk management: financial safety and sustainability aspects*, "Journal of Security and Sustainability Issues", 7(1).

Cavusoglu H., Cavusoglu H., Son J.-Y., Benbasat I., 2015, *Institutional pressures in security management: Direct and indirect influences on organizational investment in information security control resources*, "Information & Management" , 52(4).

Dillon A., Morris M., 1996, *User acceptance of new information technology: theories and models*,"Annual Review of Information Science and Technology", 31.

Hanka L., 2013, *A Doddington-féle 30-as szabály, biometrikus rendszerek megbízhatóságának statisztikai elemzése*, Tavaszi Biztonságtechnikai Szimpózium 2013, Budapest: Óbudai Egyetem.

Hanka L., Werner G., 2015, *Using the Beta-Binomial Distribution for the Analysis of Biometric Identification*, IEEE 13th International Symposium on Intelligent Systems and Informatics (SISY).

Horváth T., Kovács T., 2013, *Kockázatértékelési módszerek, azok alkalmazási lehetőségei a fizikai védelem területén*,[In:]Tavaszi Biztonságtechnikai Szimpózium 2013, Budapest: Óbudai Egyetem.

ISO/IEC, 2006, ISO/IEC 19795-1 *Information technology — Biometric performance testing and reporting* — Part 1: Principles and framework, Svájc.

ISO/IEC, 2012, ISO/IEC 19795-6:2012(E). *Information technology — Biometric performance testing and reporting* — Part 6: Testing methodologies for operational evaluation, Svájc.

Jain A.K., Fellow A.R., *Prabhakar S., 2004, An Introduction to Biometric Recognition*, "EEE Transactions on Circuits and Systems for Video Technology", 14(1).

Kliestik T., Misankova M., Valaskova K., Svabova L., 2018, *Bankruptcy prevention: new effort to reflect on legal and social changes*, "Science and Engineering Ethics", 24(2).

Kovács T., Otti C., Milák I., 2012, *A biztonságtudomány biometriai aspektusai*,[In:]A biztonság rendészettudományi dimenziói: Változások és hatások, Pécs: Magyar Rendészettudományi Társaság.

Kuril J. 2018, *Public administration for safe and secure environment: case of Slovak Republic*, "Entrepreneurship and Sustainability Issues", 5(3).

Limba T., Šidlauskas A., 2018, *Secure personal data administration in the social networks: the case of voluntary sharing of personal data on the Facebook*, "Entrepreneurship and Sustainability Issues", 5(3).

Michelberger P., Horváth Z., 2017, *Security aspects of process resource planning*, "Polish Journal of Management Studies", 16(1).

Nazareth D., Choi J., 2015, *A system dynamics model for information security management*, "Information & Management", 52(1).

Otti C., 2016, *Comparison of biometric identification methods*,IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI), Timisoara.

Otti C., 2017, *Why does it fail to operate?*[In:]Thinking Together: The economy in practice,Budapest: Óbudai Egyetem.

Oláh J., Karmazin Gy., Pető K., Popp J., 2017, *Information technology developments of logistics service providers in Hungary*. "International Journal of Logistics Research and Applications", 21(3), 332-344.

Oláh, J., Zéman, Z., Balogh, I., & Popp, J. 2018,*Future challenges and areas of development for supply chain management*, "LogForum", 14(1).

Peltier T.R., 2016, *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*, CRC Press.

Piotrowska A., Polasik M., Piotrowski D., 2017, *Prospects for the application of biometrics in the Polish banking sector*, "Equilibrium. Quarterly Journal of Economics and Economic Policy", 12(3).

Safa S.N., Von Solms R., 2016, *An information security knowledge sharing model in organizations*, "Computers in Human Behavior", 57.

Sennewald C.A., Baillie C., 2015, *Effective Security Management*, Elsevier: Butterworth-Heinemann.

Shimon M.K., 2011, *Biometrics in Identity Management: Concepts to Applications*, Norwood: Artech House.

Shpak N., Satalkina L., Sroka W., Hittmar S., 2017, *The Social Direction of Enterprises' Innovation*, "Polish Journal Of Management Studies", 16(1).

Soomro Z.A., Shah M.H., Ahmed J., 2016, *Information security management needs more holistic approach: Aliterature review*, "International Journal of Information Management", 36(2).

Springer, 2013, *Security and Privacy in Biometrics*, Springer London Heidelberg New York Dordrecht: Springer.

Stan Z., Li A.K., 2015, *Encyclopedia of Biometrics - Second Edition,* Springer New York Heidelberg Dordrecht London : Springer.

Sroka W., Cygler J., Gajdzik B., 2014, *The Transfer of Knowledge in Intra-Organizational Networks: A Case Study Analysis*, Organizacja, 47(1).

WPROWADZENIE DO SYSTEMÓW KONTROLI DOSTĘPU BIOMETRYCZNEGO DLA MENEDŻERÓW: KTÓRE WSKAŹNIKI BŁĘDU MAJA ZNACZENIE W WYBORZE?

Streszczenie: Menedżerowie w sektorze biznesowym codziennie muszą stawiać czoła problemom związanym z zarządzaniem bezpieczeństwem, a niniejszy artykuł analizuje i omawia jeden z jego segmentów, a mianowicie systemy biometryczne. Decydent otrzymuje szereg profesjonalnych danych przed wdrożeniem takiego systemu, chociaż opinia ostatecznego użytkownika będzie decydować o korzystaniu z systemu. Zgodnie z dualnym podejściem inżynier-menedżer, obecne badanie najpierw wprowadza systemy biometryczne poprzez metryki inżynierskie i koncepcje, ponieważ decydent poznaje błędy systemu poprzez te wskaźniki. Badanie podkreśla również fakt, że końcowy użytkownik jest znacznie mniej wrażliwy. Jest to jednak główny czynnik we wszystkich inwestycjach w bezpieczeństwo, niezależnie od tego, czy użytkownicy są w stanie i chcą prawidłowo korzystać z systemu. Tym bardziej w przypadku biometrycznych systemów kontroli dostępu, ponieważ algorytmy działają z różną dokładnością, a użytkownicy nigdy nie mogą być pewni, że są rozpoznawani ze 100% dokładnością. Wartości błędów dostarczone przez producentów systemów biometrycznych nie są dostępne i ponieważ są to dane algorytmiczne, różnica może wynosić kilka rzędów wielkości między faktycznie zmierzonymi wynikami. Artykuł publikuje wyniki badania ilościowego i określa indywidualny, subiektywny próg akceptacji użytkowników dotyczący błędów systemów kontroli dostępu. Na tej podstawie systemy biometryczne mogłyby być oceniane również z punktu widzenia użytkowników.
Słowa kluczowe: FRR, biometria, akceptacja użytkownika

生物识别访问控制系统为经理介绍：哪些错误指标在选择？

摘要：商业领域的管理者必须每天面对安全管理问题，本文将分析和讨论其中的一个细分领域，即生物识别系统。尽管最终用户的意见将决定系统的使用，决策者在实施此类系统之前会收到大量专业数据。继双工程师-管理者方法之后，本研究首先通过工程度量和概念介绍生物特征系统，因为决策者通过这些指标了解系统的误差。该研究还强调了这样的事实，即最终用户的敏感度要低得多。然而，这是所有安全投资的主要因素，无论用户是否能够并愿意正确使用系统。在生物识别访问控制系统的情况下更是如此，因为算法以概率运行，并且用户无法确定它们以100%的准确度被识别。由生物统计系统制造商提供的误差值不可用，并且因为这些是算法数据，所以实际测量结果之间的差异可以是几个数量级。文章发表定量研究的结果，并确定用户对访问控制系统错误的个人主观接受阈值。在此基础上，还可以从用户的角度评估生物识别系统。
关键词：FRR，生物特征识别，用户接受度