

The impact of foreign markets globalization on the price and functionality of electronic access control systems

Martin Boroš^{1,*}, Filip Lenko¹, and Andrej Velas¹

¹University of Zilina, Faculty of Security engineering, Department of Security management, Univerzitna 1, 010 26 Zilina, Slovakia

Abstract.

Research background: The research, which is the subject of the paper, is based on the global expansion of the use of electronic access control systems using biometric data for user verification. Due to the globalization of products from foreign markets to Slovakia, there is a competition between suppliers. The disadvantage is that organizations that are considering procuring an electronic access control system focus their attention only on its price. Globalization and global use have neglected the skills gap between European, American, and Asian markets.

Purpose of the article: The paper will aim to point out, through a case study, the financial and functional differences of electronic access control systems. In the case study, a comparison of three different systems with the possibility of procurement on the European, American, and Asian markets will be performed on the building - administrative building.

Methods: The article will mainly use methods such as the global method and the optimization model of the financial plan. As well as a case study, the cooperation of achieved results and analysis of possibilities of foreign markets.

Findings & Value added: The results achieved by the paper will be globally usable in the conditions of European countries. These will be the conclusions of a case study that will point to the appropriateness of choosing an electronic access control system using biometric features in a standard office building. We can also consider the creation of a project budget usable for organizations as one of the added values.

Keywords: *globalization; electronic access control systems; foreign market; economic aspect*

JEL Classification: E64; L15

* Corresponding author: martin.boros@fbi.uniza.sk

1 Introduction

Access control system is a term generally used and associated with user access to the Internet space, where this term mainly means knowledge of passwords and Wi-Fi connected, access to the corporate network and the like. With the advent of modern, smart, technology, attention has begun to shift to the protection of personal data provided within IoT systems, and the term access control systems has begun to be used with the term information access control in the system. Qiu and colleagues, in their research focused on and predicted the future development of information access control in IoT [1]. According to Qiu, it is necessary to set up an authorized user access control mechanism to access sensitive information contained in the IoT so that it complies with all legislative conditions. According to Zhang, the legislative framework for access to information is crucial in terms of the possibility of misuse of information in the IoT system. The authors describe a proposal for an integrated contractual framework, which includes integrated searches based on the assessment of incorrect access based on dynamic contract validation [2].

Within the scientific contributions and literature, there are many authors and publications focused on testing the control of access to information in the Internet space [10]. The opposite occurs in the case of object security with which the access control system is also directly connected. Even in this case, it is a verification of the identity of the user of the system and access means the physical entry of a person into a secure area. European technical standards define an access control system as a system that allows or rejects a user's request to enter or exit a secure area in a building [3].

Managing user access in the building is an important and necessary component in terms of security. The purpose of the system is to restrict the movement of persons in areas with a higher degree of protection or in an area intended only for employees. A separate category are critical infrastructure objects, the disruption or possible damage in any sense of which could have had a huge social impact. The authors of Reháč, Hromada and Loveček [4]. Dealt with the issue of resistance assessment and access elements in their research. In the article, the authors deal with a comprehensive evaluation using the CIERA method, which is designed to restore the functionality of elements after a disruptive event. It would be necessary to pay special attention to the access control system, because its non-functioning would result in unauthorized entry into the building [10].

The system of control of entrances in buildings therefore helps us with the designated authorized and unauthorized users. We could compare this approach to object-driven access to information through the roles addressed by Mundbrod and Reichert [5]. In the case of object security, there are two basic roles, namely a system user with a corrected entry and without a person authorized. It is possible to use several techniques to prove legitimacy, such as ownership - the user owns an access card, proving - the user has knowledge of the access code and property, ie biometric data. In order for this system to be of real importance, it must be supplemented by mechanical means of restraint, the task of which is to make the secured space accessible. In the absence of mechanical means of restraint, we can only speak of access systems that are currently used to monitor employee attendance. In this case, the system does not have to be supplemented by a mechanical restraint system, as it only records the time of the employee's arrival and departure from work [7]. However, there are also combined systems that are suitable for use in both cases and combine the two possibilities of use. Therefore, it is appropriate to install an access control system in the premises of companies, small or medium-sized enterprises and also in generally important buildings. In addition to gaining information, the solution can provide protection of corporate know-how, marketing strategy and other internal corporate matters, which mean the importance and position of companies in the market [11].

Despite the fact that the access control system plays an important function in terms of object security, it is still an electronic device that can be purchased virtually anywhere due to the globalization of international markets [12]. However, due to the global expansion of the markets, in addition to the benefits, the price of the product, which is felt by the customer, also affects the overall profits of individual countries [13]. Karanassou and Sala examined the impact of the distributional effects of globalization on US finances. As part of the results of their research, they propose an empirical model that assumes a 67 percent decrease in the share of labor and an 85 percent increase in income inequality caused by the globalization of markets [8, 9, 14].

As there are a large number of possibilities, it is necessary for companies that want to implement an access control system to know the financial costs associated with its acquisition. As this is a specific part of security, the requirement to implement the system must come from security personnel, and it should be cost-effective and functional [15]. The purchase of the access control system, namely due to the globalization of the international market, can be implemented from anywhere, and the number of orders from the Asian and American markets has increased rapidly in the Slovak Republic in recent years. The use of such devices has a huge financial benefit for the user, but the negative aspects of such a trade are often not considered. The disadvantages of the globalization of the international market include, in particular, the financial cost of transporting goods. In the case of an order from Asian or American online stores, the price of transporting the goods is at a minimum level, but in the case of a complaint, the customer must bear all financial and security consequences [11, 16]. Through the model situation, it is possible to realistically see the economic impact on society. Within the education of security managers, it is necessary to think not only on the effectiveness of the design of the protection system but also on the economic balance of society [17, 18]. The correct setting and function of user access to the secured area is one of the primary functions of the building protection system.

2 Methodology

To achieve the goal of the paper, we have chosen the method of the model situation, which will show the financial differences of the access control systems for the selected object. Within the financial difference, it will then be possible to see the real purchase prices of the systems that the company must have before installing the selected system. As there are currently several verification options, which were also described in the previous chapter, we decided to unify the requirements and focus on only one method using the same constraint conditions.

The model situation is focused on securing an object intended for business purposes. In the building there are three rooms to which it is necessary to restrict access and one door, which is used to enter the building itself. In total, it is necessary to secure four doors in one direction with the access control system. As part of the financial calculation of the entire system, it is necessary to include other items in the budget, such as an electric lock, reverse diodes and, last but not least, access tokens enabling an authorized user to enter.

Within the model situation, two variants will be created for the set requirements, which will then be compared from several points of view. In addition to the financial aspect from the point of view of the initial investment, other requirements will be considered, such as system extensibility and warranty service. We chose these aspects in order to express the long-term financial demands of the system.

The first variant, V1, will consist of a semi-professional system commonly available in Slovak online stores. The second variant, V2, will consist of a non-certified system from the most famous Asian online store. Transport costs will not be taken into account in the

comparison of variants, as this would significantly affect the comparison. The Asian online store is known and popular for zero shipping costs.

The total amounts of access control systems are formed by summarizing the costs of individual items and installation. For calculation purposes, we will use the standard catalogue prices of components. In the end, we will use a comparison to determine a more suitable variant and then determine the economic impact of globalization on the user.

3 Results

Variant V1 is a semi-professional and expert-recommended SYSDO system. As part of the specific assignment of the model situation, we selected the access control panel of the system. In the basic version, it enables the registration and control of access of persons for the control of one direction. It is also possible to connect four inputs to the control panel for connecting an RFID reader and the same number for connecting an exit button and monitoring the door status. The module is also equipped with alarm outputs and relay contacts to control the electric lock. A necessary part of the control panel must also be a metal box in which it will be stored.

As part of variant V1, we also propose the use of an access reader directly compatible with the SYSDO control panel. It is a reader designed for reading RFID tokens effective at a distance of up to 8 centimetres. Another integral part of the access control system is the electric lock. For design purposes, we have chosen an electric lock of standard dimensions, which is in the open position during the duration of the voltage pulse sent from the control panel based on authorized user verification. Another important part of the variant are RFID access tokens. In our case, we opted for a combination of cards and chips, so employees will be able to choose from these options based on their own preferences. Tokens should be procured when buying a system, as this is about two euros of consumables and buying one would be unnecessary. The price calculation of variant V1 is shown in Table 1.

Table 1. Calculation of first variant.

Component	Quantity pcs.	Unit price €	Total price €
Switchboard and box	1	294/15	309
Access reader	4	162	648
Electric lock	4	26	104
RFID token	20	2	40
Supply power	1	48	48
Reserve supply	1	15	15
Total			1164

From the data in Table 1 we can see that the estimated price of variant V1, without cabling, reverse diodes and installation fee is at the level of almost 1200 €. Within the total price of the system listed in Table 1, we expected to purchase ten chips and ten access cards. In the calculation, we rounded prices upwards.

The second variant of V2, as mentioned in the methodological part, consists of a product from a well-known Asian online store. The procedure for creating a variant is the

same as in the case of V1, ie it consists of the same components. Despite our efforts, we did not find the possibility of consisting of a control panel and readers, the mentioned online store has only autonomous access control systems for the Slovak market. The autonomous access control system means that the reader can only open one connected door. For the needs of the V2 variant, we chose the product with the best user rating, the system from OBO HANDS. It is a system that in the package contains an autonomous combined reader, power supply, electric lock, RFID tokens - key fobs in the number of ten. In order to maintain the uniformity of variants, we have supplemented the proposal with the same components that are not a direct part of the package. The price calculation of variant 2 is in table 2.

Table 2. Calculation of second variant.

Component	Quantity pcs.	Unit price €	Total price €
Switchboard and box	4	55	220
RFID token	10	2	40
Reserve supply	1	15	15
Total			275

The data in Table 2 show that the total purchase price of the access control system from the Asian online store is significantly lower than in the case of variant V1. Even in this case, the total amount of cabling and installation fee is not included in the total amount. In this case, it would be quite difficult to determine it, as within the V2 variant, the user will probably have to install the system himself.

As part of the mutual comparison of variants V1 and V2, we state that from a financial point of view, it is more appropriate to choose a system from the Asian online store. Due to the globalization of markets, it is possible that the V2 variant is at a level of less than € 300 for our model situation. In this case, however, price may not be the deciding factor, as there are several reasons and disadvantages to opt for variant V1. These reasons include, for example, warranty and post-warranty service. In the case of V1, the product can be claimed for a period of two years, after which there are several local companies that provide service for the selected brand. For variant V2, the warranty is questionable or non-existent, because it would be necessary to send the system or system components to the country of manufacture or the company's headquarters, which would mean that postage must be paid by the user. The level of such charges could be higher than the value of the whole system and the user runs the risk of the consignment being damaged during transport. As part of the solution of the model situation, we achieved the value of the access control system in both variants, on the basis of which companies can plan a budget for the next period.

4 Discussion

The issue of the global market of an open economy is extensive and even through a model situation we can prove that it has a direct impact on both the user and the state. It should be noted that in the case of variant V2, there is a high probability that the consignment will be detained by customs staff. In this case, the user will have to pay 20% tax or will be notified that the detained goods have been returned to the sending country.

An important fact is the fact that the product in V2 is not certified for use in the Slovak Republic. This does not mean that it cannot be used, but in the event of an insured event, the user will not be legally protected. Although the V2 system can be considered a higher level of security, as it has up to three verification methods, from a practical point of view, as a user, security manager or economist of the company, we should opt for V1.

There are many solutions to the model situation. We were able to compare the price relation of RFID readers to biometric readers, which are also popular in the Asian online store. However, in the case of biometric access control systems, we could encounter the problem that, from the GDPR's point of view, this is personal data. From the point of view of data security in the access control system, it is clearly more appropriate to use RFID technology.

5 Conclusion

The aim of the paper was to point out, through a model situation, the difference in the purchase price of the access control system, resulting from the globalization of the market and the open economy. The model situation consisted of an assignment to secure the object with an access control system. As part of the solution, we designed two variants, V1 and V2. Variant V1 consisted of a semi-professional access control system commonly available on the Slovak market, the value of which was almost € 1,200. The second variant, V2, consisted of a system available at a well-known Asian online store, the purchase price of which was almost € 300.

We compared the created variants from several points of view, while from the economic point of view it came out as a better variant V2. With the help of other aspects, such as warranty service, we pointed out the fact that the V1 variant is more suitable. Based on the results presented in the article, we can state that foreign online stores offer a really versatile range, which includes elements of the protection system. Although the price is incomparable due to the globalization of the market and the economy, it is necessary for the user to consider procuring this type of system.

This paper was supported by Grant System of University of Zilina No. 8065/2020 and project VEGA 1/0768/19.

References

1. Qiu, J., Tian, Z. H., Du, CL., Zuo, Q., Su, S., Fang, B. X. (2020). A Survey on Access Control in the Age of Internet of Things. *IEEE Internet of things journal*, 7(6), 4682-4696.
2. Zhang, Y. Y., Kasahara, S., Shen, Y. L., Jiang, X. H., Wan, J. X. (2019). Smart Contract-Based Access Control for the Internet of Things. *IEEE Internet of things journal*, 6(2), 1594-1605.
3. Bertin, E., Hussein, D., Sengul, C., Frey, V. (2019). Access control in the Internet of Things: a survey of existing approaches and open research questions. *Annals of telecommunications*, 74(7-8), 375-388.
4. Rehak, D., Senovsky, P., Hromada, M., Lovecek, T. (2019). Complex approach to assessing resilience of critical infrastructure elements. *International journal of critical infrastructure protection*, 25, 125-138.
5. Mundbrod, N., Reichert, M. (2019). Object-Specific Role-Based Access Control. *International journal of cooperative information systems*, 28(1), 1950003.

6. Catola, M., D'Alessandro, S. (2020). Market competition, lobbying influence and environmental externalities. *European journal of political economy*, 63, 101886.
7. Holla, K., Ristvej, J., Moricova, V., Novak, L. (2016). Results of survey among SEVESO establishments in the Slovak Republic. *Journal of chemical health & safety*, 23(2), 9-17.
8. Karanassou, M., Sala, H. (2020). Distributional Consequences of Technology, Trade Globalisation and Financialisation in the US. *Economic and social review*, 51(2), 275-303.
9. Agnello, L., Castro, V., Hammoudeh, S., Sousa, R. M. (2020). Global factors, uncertainty, weather conditions and energy prices: On the drivers of the duration of commodity price cycle phases. *Energy economics*, 90, 104862.
10. Lovecek, T., Vel'as, A., Kampova, K., Maris, L., Mozer, V. (2013). Cumulative Probability of Detecting an Intruder by Alarm Systems. *47th International carnahana conference on security technology (ICCST)*. Medellin.
11. Soltes, V., Stofkova, K. R., Lenko, F. (2020). Socio-economic consequences of globalization on the economic development of regions in the context of security. In T. Kliestik (Ed.), *19th International scientific conference globalization and its socio-economic consequences 2019 - sustainability in the global-knowledge economy (04026)*. Rajecke Teplice.
12. Kampova, K., Makka, K., Zvarikova, K. (2020). Cost benefit analysis within organization security management. In T. Kliestik (Ed.), *19th International scientific conference globalization and its socio-economic consequences 2019 - sustainability in the global-knowledge economy (01010)*. Rajecke Teplice.
13. Stofkova, Z., Soltes, V., Stofkova, J. (2019). Survey of the citizens digital skills in the region. In L. G. Chova, A. L. Martinez & I. C. Torres (Eds.), *12th international conference of education, research and innovation (ICERI2019)* (pp. 7127-7132). Seville.
14. Kajan, M. (2016). Globalisation of enzyme markets and influences on local markets. In T. Kliestik (Ed.), *Globalization and its socio-economic consequences, 16th international scientific conference proceedings, PTS I-V*, (pp. 800-807). Rajecke Teplice.
15. Kubas, J., Velas, A., Siser, A. (2017). Implementation of Multi-criteria Decision Making as the Method Used to Achieve Optimal Level of Security in Local Municipalities. In H. Zhang (Ed.), *4TH ICMIBI International conference on training, education, and management (ICMIBI-TEM 2017)* (pp. 371-375). Dubai.
16. Hudakova, M., Luskova, M. (2016). Global environment impacts on enterprise risk management. In T. Kliestik (Ed.), *Globalization and its socio-economic consequences, 16th international scientific conference proceedings, PTS I-V*, (pp. 694-701). Rajecke Teplice.
17. Soltes, V., Kubas, J., Stofkova, KR. (2018). Motivation of students in education in the field of security management. In L. G. Chova, A. L. Martinez & I. C. Torres (Eds.), *12th International technology, education and development conference (INTED18)* (pp. 9331-9337). Valencia.
18. Holla, K., Sventekova, E. (2019). Identifying the secondary school graduates' preferences for selecting the university and effectiveness of selected marketing tools. In L. G. Chova, A. L. Martinez & I. C. Torres (Eds.), *11th International conference on education and new learning technologies (EDULEARN19)* (pp. 2321-2326). Palma.