Economic Efficiency of the Electronic Security Systems in Security Management of Commercial Activities

Marian NASTASE[1]
Emilian Cristian IRIMESCU[2]

Abstract

The purpose of this study is to identify some general patterns of the efficiency of electronic security systems used in the security management of the commercial activities and spaces.

We also intend to identify several mathematical models to quantify the economical efficiency of electronic security systems and to determine the conditions in which these models are relevant.

In our days, security management is a key part of the economic activity (commercial also). For this reason, quantifying the economic efficiency of security systems (systems with an important role in the security management) is more a necessity and an obligation.

Being a new area of expertise, the efficiency of security systems (and general of security measures) is based on the classical way of assessing the economic efficiency, but remodelled. The old Return on Investment (ROI) will become Return on Security Investment (ROSI).

Keywords: *security management, security systems, efficiency, commercial activities, security assessment, return on investment, return on security investment*

JEL classification: M10, M15

Introduction

In this study we try to identify some tools (mathematical models) which can enable us measuring the economical efficiency of the security systems in the security management of the commercial activities. It is also important to determine the conditions under which these models are relevant for studying the economical efficiency of electronic security systems.

We try to reach our target drawing some ideas:

- Defining and presenting the electronic security systems notion;
- Defining and presenting the commercial activity form the security management standpoint;
- What is security and Risk Management for the commercial activity (spaces);

[1] **Marian NASTASE,** The Bucharest University of Economic Studies, Romania
E-mail: nastasem1@yahoo.com
[2] **Emilian Cristian IRIMESCU.** The Bucharest University of Economic Studies, Romania
E-mail: emil.irimescu@gmail.com

- Identifying some methods (models) of economic efficiency analysis for security systems used in the commercial activities security management;
- Analyzing some patterns of the economic efficiency of the security systems used in the commercial activity security management;

The importance of this study consists in finding a way to justify, from an economic perspective, why we use some specific techniques or systems in the security management of the commercial activities (spaces), and why we transform them in management tools.

1. Context

National legislation and international standards

At this moment, the Romanian law that covers the security activity (guarding and security systems), and also the security activity for commercial activities is Law no. 333 republished in 2014. There is also in force the Government decision no. 301/2012 about the methodological standards for applying Law no. 333/2003 regarding guarding of objectives, assets, values and personal protection.

Regarding the standards (including international standards) we can mention SR ISO 31000 regarding Risk Management – Principles and Guiding Lines and SR EN 31010 regarding Risk Management – Risk Assessment Techniques. SR ISO 31000 is identical with the international standard ISO 31000:2009, and SR EN 31010 is identical with the European EN31010:2010.

Conceptually, ISO 31000 fundaments the general notions of Risk Management, notions that can be applied in any activity, also in physical security. On the other hand, ISO 31010 makes the transition to the practical side of the Risk Management, treating the assessment activity (techniques, models, etc).

Internationally there are also some standards and good practice guidelines, specific to each continent. For example, in the US there is a strong security association, called ASIS international, and we also have their specific Standards and Guidelines. This is an important issue for the managers to have in mind, paying attention to the globalization process and the expansion of companies operating in different countries (Dobrea, Şerban, 2012).

If the last 40 – 50 years clearly defined Security Management as an independent activity in all kind of organizations (economical, non-profit, etc) – defined like Security Process or Security Management Process in the Business Operations – the last 10 – 20 years meant a depth refining of this area. Now, the generic security field is segmented in Physical Security (guarding, security systems, etc.) and Information Security, and each of them is also segmented in sub domains (Hayes, 1991).

2. Electronic security systems – video security systems (CCTV – Close Circuit Television)

The electronic security systems area is very wide, reaching from the classical alarm systems to the last generation security systems, like IP video surveillance systems, intelligent video systems with artificial intelligence and face recognition, specialized systems for commercial activities like Electronic Article Surveillance (EAS), professional integrated security platforms etc.

The Existing law in Romania (Law no. 333 republished in 2014) refers mostly to the classical alarm systems (Chapter no. 4 in the law 333) and omits other kind of systems, systems that are fully used in the national and international practice.

However, the Government decision no. 301/2012, in the minimal requirements chapter for specific activities (banks, commercial activities, etc) and in direct connection with the general definition for the functional areas (access, storage, transactions, etc) also indicates other systems required to be used in these cases (CCTV systems, access control, etc).

A very important field of the electronic security systems is the CCTV area (video surveillance systems). According to Sherry Harowitz, video surveillance had in the last few years a spectacular development, proportional to the information technology development and in particular to the IP technology (Harowitz, 2012). Video surveillance is one of the most important tools used by merchants in securing the commercial activity and spaces. Video surveillance is a good tool (we can say the best) in preventing and also in documenting fraud in this kind of activities (commercial activities and spaces).

Regarding the new IP video surveillance systems (Gates, 2007), we can point some particular features, such as:

- superior image quality;
- systems scalability (very useful feature for big shop networks or large commercial complexes);
- intelligent functions such as face recognition, pattern recognition, defog;

Figure 1. Analog Video Surveillance Systems vs. IP Video Surveillance Systems
Source: www.barlows-electrical.com

3. Commercial activity from the physical security approach

Related to Law no. 333 and the general regulations for the commercial activity we must underline two main ideas:

- First of all, we will take into consideration the commercial activity that runs in large spaces, with product values from low to high, and with open show spaces;
- Secondly, we will nominate the functional areas described by Law no. 333: access, transactions, storage, exposing, transfer, processing, security systems area and ATM area.

You will ask why all this are important for the efficiency of the security systems. The answer is simple: because the law in our country has specific requests regarding security systems for all these spaces. Consequently, all the investors must take into consideration the security systems for all these spaces, according to the legal provisions, and must analyze and obtain a return of their investment. It is an important field that leaders will pay attention in order to secure the functionality and performances of an organization (Nicolescu, Nastase, 2011).

In this case, the investment in security systems will take into consideration two main directions: the requirements of the law and the functional requirements, dictated by the general function rules of commercial activity.

4. Security and Risk Management for commercial activity

In presenting this concept we will start from the Risk Management notion. Why that? Because in this case, like in all others regarding security activity, we intend to deal with this issue – the risk.

What is risk? The risk notion assumes the existence of two elements: an expectation and a deviation (which can be positive or negative). In our case, the expectation can be assimilated with an accepted level of losses (thefts) and the deviation can be the accenting or reduction of the losses (Ciocoiu, 2008).

According to ISO 31000, Risk Management imposes a series of elements that must be adapted to the specific scenario. Thereby the components of the risk management process are:

- establishing context;
- identifying the risk;
- analyzing the risk;
- assessing the risk;
- treating the risk.

Applying all this to our scenario - the commercial activity - we have:

- ✓ **establishing context**: identifying the components of the internal environment (shareholders, employees, internal procedures, etc) and external environment (social and cultural environment, economic environment, geo location, etc);
- ✓ **identifying the risk**: identifying the theft risk from the exposure area,

the robbery risk in the transactions area, the theft risk in the storage area, etc.;

- ✓ **analyzing the risk**: identifying the causes that can encourage the theft actions from the storage and exposure area, identifying the causes that can encourage the robbery actions in the transactions area, etc.;
- ✓ **assessing the risk**: positioning the chances of producing the events mentioned above in three categories: unacceptable risk (actions must take whatever the costs are), intermediary risk (actions must take in consideration also the costs) and accepted risk (the risk is so low that no action is justified);
- ✓ **treating the risk**: this is the implementation of the above mentioned point: actions for minimize losses, actions for strengthening the security measures, etc.

Over all these issues there is a cyclic loop which has its origin in the living nature of any Management system. Everything is regularly monitored and reviewed.

This way we can observe that the security of commercial activities is a wide notion, including physical security, information security and also management components, like management awareness of risks, organizing operational streams in a way that does not favor losses (Beck, 2007) etc.

5. Tools in analyzing the economical efficiency of electronic security systems used in securing commercial activities

The need of measuring the economical efficiency of security politics (economical efficiency of risk reduction measures), appears from the Risk Management model as it is presented in ISO 31000, respectively the risk assessment section. An organization is sometimes in the position of choosing, depending on the desirable risk level, if it will take security measures with any cost, if it will put in balance the efficiency of these measures, or if it will ignore all the risks.

An efficient way of economic analyze of the security measures (and also of electronic security systems) is the return of investment of the electronic security systems. In this case, the return of investment will not take into consideration the amount of value brought in return by the investment, but the amount of value saved from loss. This notion was put in front for the first time in the information security (Albanese, 2006) field, and now we can apply it also in the physical security (for commercial activities for example).

Return On Investment represents the ratio between the net benefit and the costs. We can put/show this in the next formula:

$$ROI(\%) = \frac{NetBenefit}{Costs} x100$$

Starting from here, ROSI (Return On Security Investment) will take into consideration not the Net Benefit but the Capital Saved from Loss (Albanese, 2006).

To this end, Sonnenrich and Albanese propose the next formula for analyzing the Return On Investment in Security:

$$ROSI(\%) = \frac{(Average\_Loss^{*} x Risk\_Annihilation\_Rate^{**}) - Costs}{Costs} x100$$

* = average value reported for an year;

** = risk annihilation rate represents the percentage of cases when the investment is efficient.

For this formula we will have an example from the video surveillance area in the commercial activities. We will analyze the efficiency of an investment in a video surveillance system, used for the exposure, storage and transactions area, the most important and vulnerable areas according to the existing law (Government decision no. 301/2012).

In our example, the cost with the system (equipments and implementation) is about 5.000 EURO, the historical losses for an year are about 8.500 EURO (losses registered only in the areas where the system will be implemented), and the statistical rate of theft detection of this system is about 75%.

In this case, the ROSI formula will be:

$$ROSI(\%) = \frac{(8.500EUROx75\%) - 5.000EURO}{5.000EURO} x100 = \frac{6.375EURO - 5.000EURO}{5.000EURO} x100 = 27{,}5\%$$

Things would be different in a lower rate of detection, for example for 30%.

$$ROSI(\%) = \frac{(8.500EUROx30\%) - 5.000EURO}{5.000EURO} x100 = \frac{2.550EURO - 5.000EURO}{5.000EURO} x100 = -49\%$$

In the second case we observe that the investment is not longer efficient, the result being negative.

This kind of security systems was not chosen randomly. It is by far the most important system (way) of preventing theft in commercial spaces and also in documenting the events *post factum* (Beck, 2007).

Regarding other systems, the alarm systems are very good in preventing and detecting the theft attempts after business hours. Guarding is very efficient in maintaining the order in the commercial spaces, and access control systems have a limited role, mostly to control person access in some areas.

The only systems that can be compared with the video surveillance systems are the control gates (electromagnetic gates). The difference appears however from

the costs point of view, because the video surveillance systems have only an initial cost and then a very small cost for maintenance (which tends to zero), and the control gates have a direct cost category, made by the tags applied on the products.

Based on the above, the ROSI formula will be modified at Cost by counting the Initial Cost and also the Monthly Cost (in one year we will have the Monthly cost multiplied by twelve).

$$Costs = Initial\_Cost + Monthly\_Cost x 12$$

From some perspectives, we can see that the ROI and ROSI have some similar elements with cost-benefit analysis (Banacu, 2012).

Conclusions

The first conclusion that emerges referring to the economical efficiency of the electronic security systems used for the commercial spaces and activities is that it is an economical activity perfectly measurable, which can be and must be very clear delimited from the rest of the activities for an objective analyze.

The second conclusion is that ROI is a very good indicator for assessing this efficiency, and its adaptation from the information security (ROSI) is also appropriate for physical security.

The third conclusion is that the video surveillance efficiency is higher than the control gates efficiency because of the cost structure.

References

1. Albanese, J. (2006). "Return On Security Investment (ROSI) – A Practical Quantitative Model". *Journal of Research and Practice in Information Technology*, Vol. 38, No. 1, February
2. Banacu, C. (2011). *Evaluarea afacerii*. Bucuresti: Editura Tribuna Economica
3. Banacu, C. (2012). *Analiza cost-beneficiu in proiectele de investitii - metode si tehnici de lucru. Bucuresti: Editura Tribuna Economica*
4. Beck, A. (2007). *Effective Retail Loss Prevention: 10 Ways to Keep Shrinkage Low*. Leicester : University of Leicester
5. Ciocoiu, C. (2008). *Managementul riscului. Teorii, practici, metodologii*. Bucuresti: Editura ASE
6. Dobrea, C., Şerban, E. (2012) *Analysis of Foreign Direct Investment Determinants at the Level of a County in Romania*, Economia. Seria Management, Volume 15, Issue 1
7. Gates, M. (2014). *Security Management*, March 2014: The Perks of IP Video, ASIS International, Virginia
8. Harowitz, S (2012). *Security Management*, December 2012: Surveillance System Technology Trends, ASIS International, Virginia

9. Hayes, R. (1991). *Retail Security and Loss Prevention*. Woburn: Butterworth-Heinemann
10. Jones, P.H. (1990). *Retail Loss Control*. London: Butterworth
11. Nicolescu, O., Nastase, M. (2011). *Minidictionar de management*. Manageri si lideri, Bucuresti: Editura Pro Universitaria
12. ***SR ISO 31000:2010 – *Managementul Riscului. Principii şi linii directoare*, Asociaţia Romana de Standardizare din România (ASRO), Bucureşti
13. ***SR ISO 31010:2010 – *Managementul Riscului. Tehnici de evaluare a riscului*, Asociaţia Romana de Standardizare din România (ASRO), Bucureşti
14. ***Legea 333/2003 republicată în 2014
15. ***HG 301/2012 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor