Indicators for Determining Collaborative Security Level in Organizational Environments

Cătălin SBORA
Academy of Economic Studies of Bucharest
catalin.sbora@gmail.com

This paper presents the concept of security management through collaboration highlighting the limitations for conventional security management systems and the challenges in maintaining an acceptable level of security in organizational environments. There are presented four different aspects regarding information security, aspects that involve malware threats, perimeter protection, exploiting vulnerabilities and detection of vulnerabilities. Analyzing a set of experiments regarding malware protection the paper concludes the need to improve existing protection systems by standardization and collaboration. A set of indicators for measuring the level of security by considering each of four aspects, is presented and analyzed, highlighting the benefits obtained by using collaboration in the process of managing information security. A qualitative indicator is built based on the four aspects of security presented in the paper.
Keywords: *Collaborative Security Management, Organizational Environment, Security System, Malware Threats, Security Indicator, Perimeter Protection, Intrusion Prevention*

1 Introduction

Collaboration in computer systems is closely linked to the evolution of distributed systems and the evolution of communication systems. The fact that computer systems are increasingly used as support for collaboration within business operations, provides the following benefits:

- operations are conducted in a rapid and controlled pace through automation and communication channels
- there is a possibility to observe the weaknesses of the business process in relation to the relationships between collaborators
- the possibility of establishing a historical database used to forecast trends for short and medium term
- business continuity depends less on the employees migration

The benefits of information systems depend to a great extent of information and access to information. It is important for the information to be accessible and consistent with the initial state. Altering information in an unauthorized manner and not based on a real context, reduces the effectiveness of information systems in business processes to the point where it affects an organization's ability to carry out daily activities. It is important that information and access to information to be managed in an appropriate manner so that the computer system that relies on this information to be considered reliable. Issues of confidentiality, integrity and availability of information are being considered in the notion of information security. Information security management operations are represented by mechanisms and techniques used for achieving information security. Information security management in a collaborative computing environment is often a difficult task because people tend to neglect aspects of cybersecurity focusing on achievement of short-term business goals. To prevent unpleasant situations where important information is losing its confidentiality state or it is fraudulently altered, requires the use of computer systems to identify situations that present security risks and block human actions that led to such a situation or issue warnings with respect to the situation. If in small organizations information security is relatively easy to manage and do not necessarily require well-established management processes for managing security, in large and very large organizations information security management is a necessity due to the diversity and variety of

DOI: 10.12948/issn14531305/18.4.2014.12

environments across the organization. Considering computer security in the global context, the companies are facing common threats coming from outside the company and also particular threats that are specific to each organization. Information security management through collaboration aims to improve security processes that manage threats coming from outside. Using collaboration in this situation makes sense in the context of the organizations using information systems to support daily activities are connected to the Internet, either directly or indirectly. By connecting to a common environment there will be threats that are common to all of the organizations, so there will be a general interest for all the organizations with legitimate activities to combat these threats. The common goal that motivates collaboration, in this case, is to prevent and combat cyber-attacks. Collaboration at this level consists on sharing information on the attacks encountered in the organization and sharing information on security management techniques. Sharing information on cyber-attacks encountered in an organization allows employees to take appropriate measures to manage the types of attacks found in other organizations. Such an approach will speed up the response to cyber-attacks significantly reducing the financial damage globally.

2 Aspects of information security

Regarding cybersecurity, depending on its specific, each organization has different objectives involving different aspects of information security. Issues considered to be the most common and that need to be addressed in each organization are related to malware threats, perimeter protection, exploiting vulnerabilities and detect vulnerabilities.

Malware is the item most used by cybercriminals to gain unauthorized access to data, information alteration or destruction. At the industry level anti-malware solutions are based on identification by using a database of signatures and heuristic detection by using algorithms based on the identification of behavioral patterns. Heuristic detection technology is relatively new and it still has shortcomings that must be addressed, these problems relate to the high rate of misidentification of malware. However using this method of detection in combination with signature-based detection shows a considerable advance in antivirus technologies. Since the number of malware increases by the day, updating signature databases must keep pace with the rate of occurrence of malware. According to [1] in 2013 occurred about 30 million new malware with a daily average of about 82,000 applications. Under these conditions, the problem for the malware solutions manufacturers is to keep pace with the emergence of new malware. The large number of malware to be recorded in the database for antivirus products is very high and often exceeds the resources available for each antivirus manufacturer. To check the speed of response of antivirus solutions [2] presents a study that demonstrates the inability of the manufactures to update the virus signature database in real-time. The steps in the verification tests were:

1. A database containing malware with samples identified in the last twenty-four hours was downloaded from the web address http://www.virussign.com
2. There were chosen ten random samples
3. Each of the ten selected samples was sent for analysis to www.virustotal.com, verifying whether the anti-virus databases used for the analysis have been updated in the last 24 hours
4. It was made a statistical table to track samples which are detected and antivirus that detected them
5. The results are being analyzed in two directions:
   a. The average detection level antivirus solutions
   b. Average antivirus detection for each component separately

As a result of experiments conducted it was diagram of Figure 1 illustrates the rate of detection for each virus tested.

DOI: 10.12948/issn14531305/18.4.2014.12

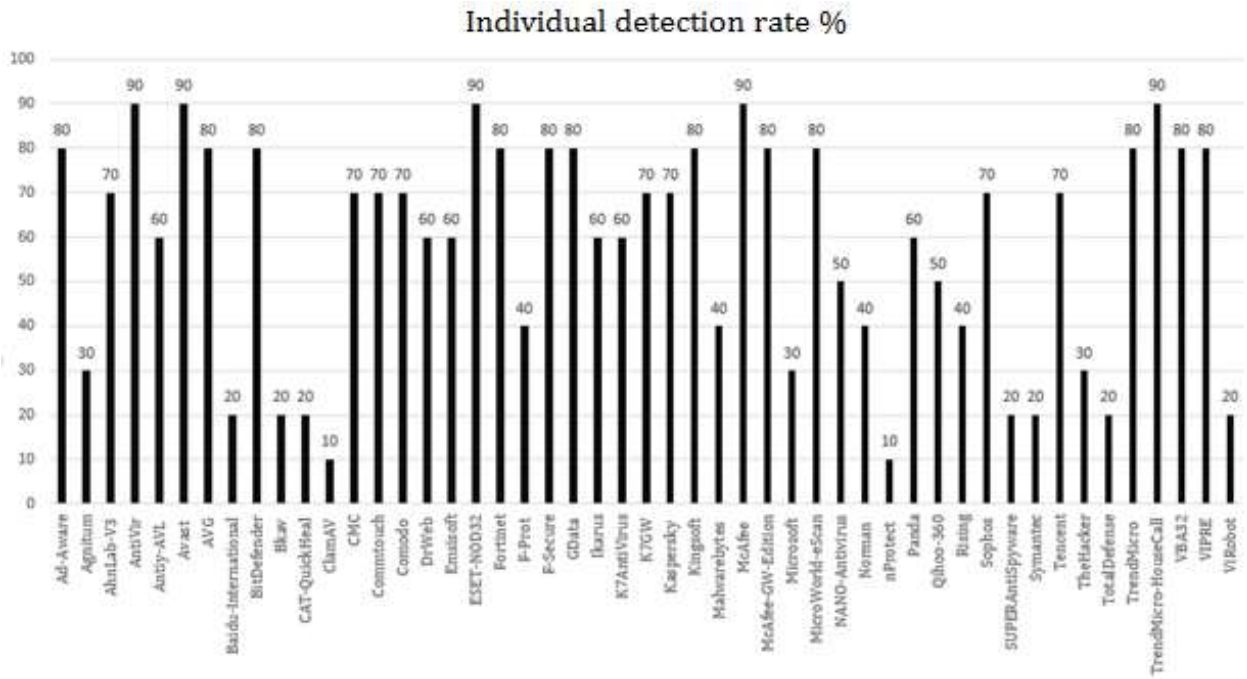

Fig. 1. Graphical representation for detection rate on antivirus components used in the experiment [2]

Note that the detection rate varies between 10% and 90%, and no component was able to identify 100% of malware items. The experiments were conducted with samples of malware identified and available for analysis. It is noted that the source used to obtain malware samples provide samples for analysis for the following laboratories: Avast, Avira (AntiVir), BitDefender, Comodo, DrWeb, McAfee, Kaspersky, Microsoft, Norman, Rising, Sophos, Symantec. And if we analyze the data obtained is observed that some of the companies on the list of beneficiaries for the samples used in the test had a detection rate of only 20%. Analysis of data obtained during the verification reveals that the results obtained are complementary in the sense that for any sample analyzed at least one antivirus detects it as being a malware sample. In terms of collaboration between antivirus manufacturers detection rate is considerably improved. The fact that none of the antivirus components analyzed manages to deliver the promised results indicate that there are still things that need to be changed for the entire sector. The first thing that helps is to standardize the development and performance improvement. Standardization and unification of virus signature database allows a much higher speeds than the current situation where basically the same malware samples are analyzed by each manufacturer. This can only be achieved by establishing an international collaboration between the manufacturers of antivirus solutions. Establishing a base of common malware without additional measures, leads to the demotivation of those who contribute to the update process, meaning that antivirus manufacturers lose their motivation when they know that their product is updated anyway, without them having to contribute directly. As in any collaborative process, those involved must have something to gain in order to maintain interest in the collaborative process. In these conditions a mechanism of direct remuneration is required such that the remuneration commensurate with their involvement in the process of updating the signatures database. The mechanism will keep the motivation for the manufactures to continue updating the common base signatures. This is because those who contribute more will be remunerated by those who participated less in the process of updating. This mechanism has the potential to eliminate small players in the

DOI: 10.12948/issn14531305/18.4.2014.12

market of antivirus component manufacturers, because they cannot afford to remunerate those who contribute more, but at the same time it will increase efficiency standard, yielding to an antivirus component that is far superior to what is currently available on the market. Collaborative approach solves the problem of updating signatures database in a rapid manner. In 2012, iMPERVA conducted a study on the effectiveness of antivirus components using emerging samples and concluded that in the case of relatively new samples, detection rate is about 5%, which is extremely low but quite normal considering the principle of operation of these components. While pursuing the detection rates for antivirus products was found that the period required for at least one of the tested product to reach a 100% detection on samples used was about four weeks, which is a time extremely long in a dynamic environment in which information travels very quickly. This report confirms that manufacturers of antivirus solutions are currently overwhelmed by the large amount of malware appearing every day, but it also reinforces the idea that cooperation is necessary for the industry. As can be seen the efficiency of antivirus components is strongly dependent on the timeliness of the signatures used, resulting that in a real environment is important that these signatures be collected from antivirus vendor in a short time. This is not necessarily a problem when it comes to a small number of devices, but when considering an infrastructure using from several hundred to several thousand devices, the update process is a complex task that requires attention and appropriate management. Factors that cause problems in large computing infrastructures are:

- Bandwidth used for retrieving updates
- Excessive use of processing resources
- Various errors that prevent correct update for the virus signature database

Process safety management must take into account these factors and include measures such as: planning update times, determining a hierarchy of update to reduce the bandwidth usage, by using internal servers to update and by using the management console to allow tracking of the upgrade process and also tracking the errors and warnings that occurred during the update.

Perimeter protection mechanisms are based on using rules to protect the perimeter. These rules cover most of the times the communication ports that are allowed, communication ports are blocked, IP addresses that are blocked and not allowed under any circumstances.

If for the anti-malware solutions getting the optimum performance from the protection modules depends more on the manufacturer, in the case of security solutions for perimeter protection getting optimal performance depends largely on the technical knowledge of the end user as well as its ability to create protection rules that take into account the source address, destination address, protocol used to transport level of the OSI model, as shown in Figure 2.

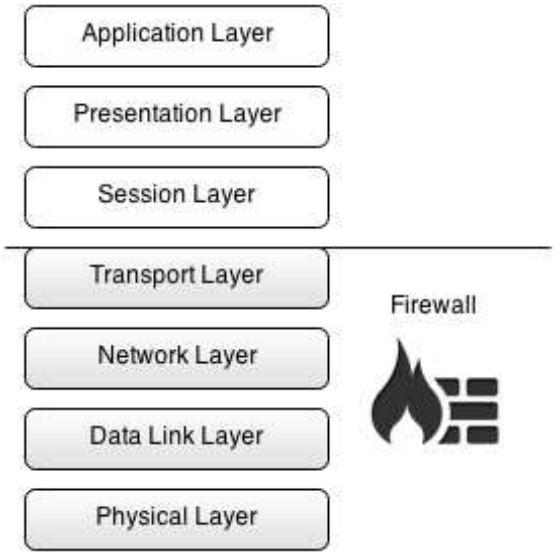

Fig. 2. Applying Firewall rules on OSI model

Intrusion prevention systems act mostly at higher levels of the OSI model by analyzing the content according to the protocol used in the application context. At this level, content analysis is carried out in detail enabling content structure validation, identifying attempts to exploit vulnerabilities in existing software applications and identifying patterns of information deemed to be sensitive.

DOI: 10.12948/issn14531305/18.4.2014.12

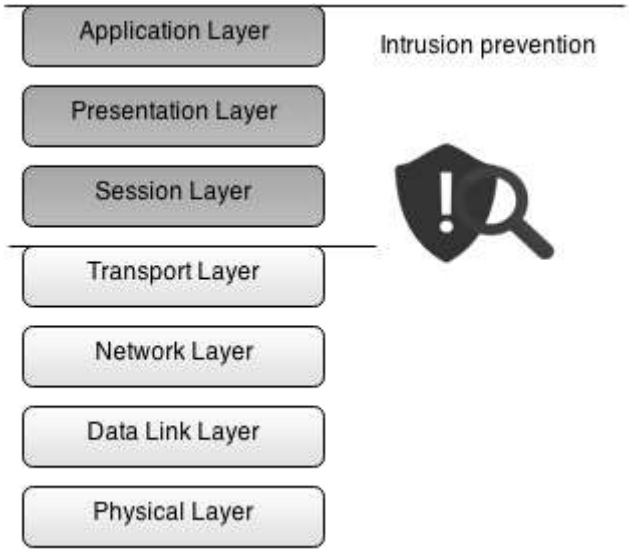

Fig. 3. Applying Intrusion Prevention rules on OSI model

The efficiency of these systems is also directly influenced by user-created rules which contribute significantly to the correct functioning of the system. When the coverage of the rule sets is higher the security level is also high. In these conditions for security components based on sets of rules, security management requires effective management of security policies so that they can be updated in a short time after the flaws were detected.

Considering the characteristics of the security components and knowing that each component covers only certain aspects of the security it cannot be estimate the overall effectiveness of a security component relative to the overall cyber security, because cyber security has different aspects, depending on the context in which this term is being used. Instead the effectiveness of the security components relative to security issues that they cover are being monitored. Moreover, in a security system maximum efficiency can be achieved when security components cover complementary aspects of the security issues specific to the environment that the security system has to protect. As a consequence in a safe computing environment it is important the effectiveness of the overall security system and not necessarily the efficiency of each component.

3 Indicators for security aspects

Considering the security aspects discussed in the previous section there are defined indicators to measure the level of security in relation to every aspect in part aiming at highlighting the collaborative contribution. Benefits received from collaborators for a security management system are translated in security rules or new templates identifying new types of attacks, to help improve the security system.

Malware protection security indicator is calculated based on the following factors:

- Number of security rules to block malicious activities
- Estimated number of malware active
- Number of blocked malware attacks
- Total number of attacks
- Number of security rules to block malicious activities

Consider the set MR, comprising all the security rules for blocking malicious activities at the organizational level. The set MR decomposes into the subsets MRA and MRD, where MRA represents the set of security rules used for blocking malicious activities covered in the database provided by antivirus solution used and the MRD is the set of locally defined security rules for blocking malicious activities.

DOI: 10.12948/issn14531305/18.4.2014.12

The indicator for establishing the coverage of the security rules in malware protection is given by (3.1)

$$ISMe = \begin{cases} \frac{NTs + NRM}{NEM}, & NEM > 0 \\ 1, & NEM = 0 \end{cases} \quad (3.1)$$

where:
ISMe – the indicator for establishing the coverage of the security rules for malware protection
NTs – the total number of rules covered in the database provided by antivirus solution used, *NTs* = cardinal (MRA)
NRM – number of rules defined for blocking malicious activities, *NRM = cardinal (MRD)*
NEM - estimated number of malware applications spread around the world

Compared to the practical context for NTs, NRM and NEM the following properties are defined:

$$NTS, NRM, NEM \in \mathbb{N};$$
$$NTS + NRM \leq NEM;$$

In this context ISMe ∈ [0, 1].
To determine the success rate in blocking malware attacks the ISMf indicator is being used and is given by (3.2)

$$ISMf = \begin{cases} \frac{NMb}{NTAm}, & NTAm > 0 \\ 1, & NTAm = 0 \end{cases} \quad (3.2)$$

where:
NMb - number of blocked malware attacks
NTAm - total number of malware attacks
Compared to the practical context in which the values are set for NMb and NTAm the following conditions have to be met:
NMb, NTAm ∈ ℕ
NTAm ≥ NMb
In this context ISMf ∈ [0, 1].
Considering that the indicators ISMe and ISMf represent aspects of security level in terms of malware protection, the indicator of arithmetic average is used to obtain the aggregate indicator for malware protection, *Ism*, according to expression (3.3).

$$Ism = \frac{ISMe + ISMf}{2} \quad (3.3)$$

where:
ISMe – indicator to establish the coverage of security rules for malware protection
ISMf – indicator to determine the success rate in blocking malware
According to the way the ISMe and ISMf indicators are being defined, the maximum value that can be achieved is 1 and the minimum value is 0. It follows that *Ism*, being the average of the two indicators, belongs to the interval [0, 1]. Value of 0 for *Ism* is being interpreted as representing the situation in which security systems are unable to provide protection against malware, and the value 1 is interpreted as being the ideal situation in which security systems are capable of providing protection against malware. Rules for blocking malicious activities represent the component that is influenced by the collaboration. It is noted that this component changes the security level in a direct proportion. When the number of rules is higher the security level increases. In a collaborative management process, the set of the security rules for blocking malicious activities, MRD, decomposes according to (3.4).

$$MRD = MRDp \cup MRDc \quad (3.4)$$

where:
MRDp – the set of security rules for blocking malware activities, defined within the organization
MRDc – the set of security rules received from contributors used for block malicious activities
From relation (3.4) and considering MRDp and MRDc as disjoint sets, results: cardinal

DOI: 10.12948/issn14531305/18.4.2014.12

(MRD) = cardinal (MRDp) + cardinal (MRDc).

Whether NRMp = cardinal (MRDp) and NRMc = cardinal (MRDc), it results that the number of security rules to block malicious activities, NRM, can be expressed as:

$$NRM = NRMp + NRMc.$$

To measure the benefits on malware protection received from collaborators MRB indicator is being used and it is defined by (3.5)

$$MRB = \begin{cases} \frac{NRMc}{NRM}, & NRM > 0 \\ 0, & NRM = 0 \end{cases} \quad (3.5)$$

where:

MRB – benefits received from collaborators on malware protection rules

NRMc – number of rules for the protection malware received from contributors

NRM – total malware protection rules

Because NRM, NRMc $\in \mathbb{N}$ and NRMc $\leq$ NRM the MRB indicator belongs to the interval [0,1].

Value of 0 for MRB shall be considered as representing the situation where no rule for malware protection is taken from collaborators and the value 1 is interpreted as the situation in which all malware protection rules are taken from collaborators.

Security level indicator based on existing vulnerabilities is defined according to the following factors:

- Number of rules to detect vulnerabilities
- Estimated total number of vulnerabilities
- Number of blocked attempts to exploit existing vulnerabilities
- Total number of attempts to exploit vulnerabilities

It is to be considered the set, comprising all the rules for detecting security vulnerabilities in software applications on the organizational level. MRV set decomposes into subsets MRVP and MRVC, where: MRVP represents the set of rules for identifying security vulnerabilities, defined locally, and MRVC is the set of rules for identifying security vulnerabilities, received from collaborators.

The indicator used to establish the coverage of the rules for identifying security vulnerabilities, ISVe, is given by (3.6)

$$ISVe = \begin{cases} \frac{NAp + NAc}{NEV}, & NEV > 0 \\ 1, & NEV = 0 \end{cases} \quad (3.6)$$

where:

NAp – number of own audit rules with NAp = cardinal (MRVP)

NAc – number of rules received from collaborators, for identifying vulnerabilities, NAc = cardinal (MRVC)

NEV – total number of estimated vulnerabilities

Considering the practical values are set for *NAp*, *NAc* and NEV are considered the following conditions:

$$NAp, NAc, NEV \in \mathbb{N};$$
$$NAp + NAc \leq NEV;$$

In this context ISVe takes values in the interval [0, 1].

To determine the success rate in blocking attempts to exploit existing vulnerabilities using ISVf indicator, given by (3.7)

$$ISVf = \begin{cases} \frac{NEb}{NTEi}, & NTEi > 0 \\ 1, & NTEi = 0 \end{cases} \quad (3.7)$$

where:

NEb – number of blocked attempts to exploit vulnerabilities

NTEi – the total number of attempts to exploit various vulnerabilities

Compared to the practical values are set for NEb, resulting muffler following conditions:

$$NEb, NTEi \in \mathbb{N}$$
$$NTEi \geq NEb$$

In this context ISVf belongs to [0, 1].

ISVe and ISVf indicators represent aspects of security level in terms of the existence of vulnerabilities in the software. Using ISVe and ISVf, in conjunction with arithmetic average an aggregated indicator is being defined as *Isv* according to expression (3.8)

$$Isv = \frac{ISVe + ISVf}{2} \quad (3.8)$$

where:

ISVe – indicator to establish the coverage for the rule used for identifying security vulnerabilities

ISVf – indicator to determine the success rate

DOI: 10.12948/issn14531305/18.4.2014.12

in blocking attempts to exploit existing security vulnerabilities

According to how ISVf and ISVe are defined, the maximum value that can be achieved is 1 and the minimum value is 0, it results that the maximum value for ISVe + ISVf is 2, and the minimum value is 0. From previous observations that the minimum value for *Isv* is 0 and the maximum value is 1, *Isv* belongs to the interval [0, 1].

A value of 0 for *Isv* shall be interpreted as representing the situation in which computer systems presents a high number of vulnerabilities and security systems are unable to provide protection against exploitation of these vulnerabilities. Value 1 for *Isv*, shall be considered as representing the ideal situation where systems have a number of vulnerabilities which tends to 0 and the attempts to exploit existing vulnerabilities were successfully blocked by the security system.

Indicator to measure the benefits received from collaborators on identifying vulnerabilities, VRB, is given by (3.9)

$$VRB = \begin{cases} \frac{NAc}{NEV}, & NEV > 0 \\ 0, & NEV = 0 \end{cases} \quad (3.9)$$

where:

VRB – indicator for the total benefits received on identifying vulnerabilities

NAc – number of rules for identifying vulnerabilities, received from collaborators

NEV – total number of estimated vulnerabilities

considering that:

$$NAc, NEV \in \mathbb{N};$$
$$NAc \leq NEV;$$

In this context VRB takes values in the interval [0, 1].

Value of 0 for VRB be shall be interpreted as representing the situation where no rule for auditing vulnerabilities have been taken from collaborators and the value 1 shall be interpreted as the situation in which all the rules for vulnerabilities were taken from collaborators.

Security level indicator based on intrusion prevention refers to the extent that the security system has the ability to inspect traffic in the communication channels and to identify the information that is dangerous for the computer system. In a collaborative environment, this indicator is influenced by the following factors:

- Number of rules to prevent intrusions
- Estimated number of threats used for intrusion
- Number of attacks blocked by the intrusion prevention system
- Total number of intrusion attacks

Considering the set MP, comprising all the rules to prevent intrusions. The MP set decomposes into subsets MPP and MPC, where: MPP is the set of the rules defined internally for intrusion prevention and MPC represents the rules received from the collaborators that are being used for intrusion prevention.

The indicator for establishing the coverage of the security rules for intrusion prevention is represented by ISPe and it is given by (3.10)

$$ISPe = \begin{cases} \frac{NRPp + NRPc}{NEP}, & NEP > 0 \\ 1, & NEP = 0 \end{cases} \quad (3.10)$$

where:

NRPp – number of internally defined rules to prevent intrusions, NRPp = cardinal (MPP)

NRPc – number of rules received from collaborators to prevent intrusion, NRPc = cardinal (MPC)

NEP – estimated number of threats used for intrusion

Considering the practical context in which the values for NRPp, NRPc and NEP are being set, it results that the following conditions are met:

$$NRPp, NRPc, NEP \in \mathbb{N};$$
$$NRPp + NRPc \leq NEP;$$

In this context, ISPe indicator takes values in the interval [0,1].

To determine the success rate in blocking intrusion attempts, the ISPf indicator shall be used, in the conditions where the indicator is given by (3.11)

$$ISPf = \begin{cases} \frac{NIPb}{NIP}, & NIP > 0 \\ 1, & NIP = 0 \end{cases} \quad (3.11)$$

where:

DOI: 10.12948/issn14531305/18.4.2014.12

NIPb –the number of intrusion attacks blocked by the security system
NIP – total attacks of intrusion
Considering to the practical context in which the values for NIPb, NIP are set it results that the following conditions have to be met:

$$NIPb, NIP \in \mathbb{N}$$
$$NIP \geq NIPb$$

In this context ISPf belongs to [0, 1].
ISPe and *ISPe* indicators are aspects of security level in terms of susceptibility to attacks of intrusion. Using ISPf and ISPe, in conjunction with the indicator of arithmetic average it results an aggregated indicator for intrusion prevention security, *Isp*, given by (3.12).

$$Isp = \frac{ISPe + ISPf}{2} \quad (3.12)$$

According to how ISPf and ISPe are defined, the maximum that they can achieve is 1 and the minimum value is 0, it results that the maximum value for ISPe + ISPf is 2 and the minimum value is 0. From previous observations the minimum value for *Isp* is 0 and the maximum value is 1, so that *Isp* takes values in [0, 1].
Value of 0 for *Isp* shall be interpreted as representing the situation in which computer systems present a large number of security breaches and security systems are unable to provide protection for blocking access to information through these breaches. Value 1 for *Isp*, shall be considered as representing the ideal situation where the systems have a very low number of security breaches and the attacks attempting to exploit the existing breaches were successfully blocked by the security system.
The indicator for determining the benefits received from the collaborators, relative to intrusion prevention, PRB is given by (3.13)

$$PRB = \frac{NRPc}{NEP} \quad (3.13)$$

where:
PRB – the total benefits received from collaborators relative to intrusion prevention system
NRPc – number of rules received from collaborators that are being used to guard against intrusion attacks
NEP – estimated number of threats used for intrusion
considering that:

$$NRPc, NEP \in \mathbb{N};$$
$$NRPc \leq NEP;$$

In this context indicator PRB takes values in the range [0, 1].
Value of 0 for PRB shall be interpreted as representing the situation where no rule to prevent intrusion was taken from collaborators and the value 1 is interpreted as the situation in which all the rules to prevent intrusions were taken from collaborators.
The indicator for determining the security level relative to the perimeter protection system is determined by the following factors:

- Number of rules for perimeter protection
- Total perimeter protection rules expected to be required for full protection
- Number of attacks blocked by perimeter protection system
- Total perimeter penetration tests

It shall be considered the set MF, comprising all the rules for perimeter protection. The set MF decomposes into subsets MFC and MFP where: MFP is the set of rules for protecting the perimeter, defined within the organization, and MFC is the set of rules for protecting the perimeter, received from contributors.
Indicator for determining coverage of security rules in terms of perimeter protection, ISFe is given by (3.14)

$$ISFe = \begin{cases} \frac{NRFp + NRFc}{NIF}, NIF > 0 \\ 1, NIF = 0 \end{cases} \quad (3.14)$$

where:
NRFp – the number of the rules defined internally used for perimeter protection system, NRFp = cardinal (MFP)
NRFc – the number of rules received from collaborators used for perimeter protection system, NRFc = cardinal (MFC)
NIF – total firewall rules considered necessary for a full coverage of the needs
provided that:

$$NRFp, NRFc, NIF \in \mathbb{N}$$
$$NRFp + NRFc \leq NIF$$

DOI: 10.12948/issn14531305/18.4.2014.12

In this context ISFe receives values in the interval [0, 1].

For determining the success rate when blocking the penetration of the perimeter attacks, the indicator ISFf is used and is given by (3.15)

$$ISFf = \begin{cases} \frac{NAFb}{NAF}, & NAF > 0 \\ 1, & NAF = 0 \end{cases} \quad (3.15)$$

where:

NAFb - number of attacks blocked by perimeter protection system

NAF - the total number of attacks relative perimeter protection system

provided that:

$$NAFb, NAF \in \mathbb{N}$$
$$NAFb \leq NAF$$

In this context, it is obvious that ISFf ∈ [0, 1].

ISFe and ISFf indicators represent aspects of security level in terms of perimeter protection. Using ISFe and ISFf, in conjunction with arithmetic average indicator it results the aggregated indicator for perimeter protection, *ISF*, given by (3.16)

$$Isf = \frac{ISFe + ISFf}{2} \quad (3.16)$$

According to how ISFf and ISFe are defined, the maximum value that they can achieve is 1 and the minimum value is 0, it results that the maximum value for ISFe + ISFf is 2, and the minimum value is 0. From previous observations it can be stated that the minimum value for *Isf* is 0 and the maximum value is 1, so that *Isf* belongs to the interval [0, 1]. Value of 0 for *Isf* shall be interpreted as the situation in which security systems are unable to provide protection to block access to the areas to be protected. Value 1 for *Isf*, shall be interpreted as representing the ideal situation where the rules for perimeter protection security system covers all the needs and all attempts to penetrate the perimeter were successfully blocked by the security system.

To determine the benefits from collaboration relative to perimeter protection system, the indicator FRB is being used, and FRB is given by (3.17)

$$FRB = \frac{NRFc}{NIF} \quad (3.17)$$

where:

FRB - benefits received by collaborators relative to the firewall

NRFc - number of rules received from collaborators, used for firewall

NIF - total firewall rules considered necessary for a complete coverage of needs given that:

$$NRFc, NIF \in \mathbb{N}$$
$$NRFc \leq NIF$$

In this context FRB belongs to [0, 1].

As can be observed to determine the level of security indicators are determined on the basis of collaborators contribution. Benefits received from collaborators to improve security are determined by (3.5), (3.9), (3.13), (3.17) having a positive impact on the level of security in an organization.

4 Aggregated security indicators

Security level is influenced directly and equal by all of the four indicators discussed in section three. Assuming that the four security indicators are independent of one another, the premise for developing aggregate indicator *Is* as their average, is created.

Aggregate indicator for the level of security within the organization, *Is*, is given by (4.1).

$$Is = \frac{Ism + Isv + Isp + Isf}{4} \quad (4.1)$$

where:

Is – aggregate indicator for the level of security within an organization

Ism – security level indicator reported in malware protection

Isv – security level indicator generated based on existing vulnerabilities

Isp – security level indicator based on intrusion prevention

Isf – security level indicator based on security perimeter protection mechanism

The aggregated indicator for the level of security, *Is*, is determined based on the four aspects because it aims to determine the impact of inter-organizational collaboration and thus there are analyzed the issues involved directly by collaboration process.

Security indicators are obtained on the basis

DOI: 10.12948/issn14531305/18.4.2014.12

of statistical data and therefore their accuracy is given by the size of the sample base. The more data are sampled from more diverse environments the more security indicators have a higher precision and therefore the security level is estimated with a higher accuracy.

Security indicators are determined as a value between 0 and 1, 0 being minimum and one maximum value.

It is considered that the indicator, *Is*, is being monitored in time, and its values are sampled in a set consisting of n elements $\xi = \{Is_0, Is_1, ..., Is_n\}$. Starting from [3], the security level is expressed as (4.2)

$$SP \approx \frac{1}{n}\sum_{i=0}^{n} Is_i \qquad (4.2)$$

For an easy interpretation of the SP indicator a template function, SL, is defined. The function aims to establish a correspondence between the numerical value of SP and a qualitative level for the efficiency of the security systems. In the event that SL is a function defined on the interval [0, 1], and this range is divided into four subintervals: [0, T1], [T1, T2], [T2, T3], [T3 1], which are available in correspondence with qualitative levels defining the function by:

$$SL\text{: } [0, 1] \rightarrow \{\text{Very weak, Weak, Good, Very Good}\}$$

$$SL(x) = \begin{cases} Very\ Weak, & 0 \le x \le T1 \\ Weak, & T1 < x \le T2 \\ Good, & T2 < x \le T3 \\ Very\ Good, & T3 < x \le 1 \end{cases}$$

where:

T1 - upper threshold for which it is considered that the security level is extremely low, T1 ∈ [0,1]

T2 - upper threshold for which the security level is considered to be low

T3 - upper threshold for which security level is at an acceptable level

Assuming the use of thresholds T1 = 0.25, T2 = 0.5, Q3 = 0.75, for the SL function a new indicator generated by SP, denoted by SL' is obtained. SL' is represented by (4.3) and the graphical representation is shown in Figure 4.

$$SL' = \begin{cases} Very\ Weak, & SP \in [0, 0.25] \\ Weak, & SP \in (0.25, 0.5] \\ Good, & SP \in (0.5, 0.75] \\ Very\ Good, & SP \in (0.75, 1] \end{cases} \qquad (4.3)$$

Fig. 4. Correlation between security level SP and the qualitative indicator SL' [2]

DOI: 10.12948/issn14531305/18.4.2014.12

It should be noted that in the above definition, SL' is an initial definition which has not been validated in a real environment. To validate or adjust the thresholds for this indicator a correlation tracking is needed for at least one year of evolution for SP security level relative to the number of security incidents. Monitoring should be carried out in several computer environments with high structural diversity. On the basis of experiments, the four intervals initially having the same size are adjusted in such a way that they will reflect as accurate as possible the observations from the real environments. In the case where the number of experiments is very high it is considered the usage of Gauss's normal distribution for establishing the correlation between the SP indicator and the levels of quality.

5 Conclusions

In the context where people are becoming more and more connected through information technology and the geographical boundaries are virtually erased, organizations have extended their operations worldwide, increasing the need of collaboration. Collaboration is encouraged by the evolution of technology which allows employees to interact much easier and with increased productivity. Collaboration, however, raises information security issues generated by the heterogeneous environments in which information travels. Considering the fact that the computerization level has increased for most of organizations, information has become an important asset, thereby is important to be protected. The loss, the leak or the unauthorized alteration of the information in most cases has a huge negative impact on the daily activities within an organization, leading to situations where the activity is blocked and the financial loses are huge. Mechanisms and procedures for managing information security have already been developed, however the dynamics of technology and cybercrime makes the conventional means of protection to become deprecated. New means of enforcing security mechanisms and techniques are required and using collaboration for information security management is an option that must be explored. Within an organization there is permanent need of awareness regarding information security and the exposure of the organization to the existing cyber threats. This paper present a series of indicators that can be useful when assessing the security level inside an organization by allowing a correlation between a numerical computed value and qualitative levels. Having a qualitative representation of the information security allows the non-technical executives to better understand where they stand from the information security perspective so they can take better decisions regarding the way the data within the organization should be handled. As the technology and the society evolves there is strong dependency created between organizations and information. The importance of information security becomes fundamental for most of the organizations thereby new and innovative approaches are required to keep the pace with the existing cyber threats.

References

[1] Panda Security Report (2014, November 21), available online at: http://press.pandasecurity.com/wp-content/uploads/2010/05/PandaLabs-Annual-Report_2013.pdf

[2] C. Sbora, PhD Thesis Collaborative Security Management in Distributed Systems, public presentation on October 24, 2014

[3] A. J. A. Wang - Information Security Models and Metrics, ACM-SE 43 Proceedings of the 43rd annual Southeast regional conference, Volume 2, ACM New York, 2005, pp 178-184, ISBN:1-59593-059-0

DOI: 10.12948/issn14531305/18.4.2014.12

Catalin SBORA graduated the Faculty of Automatics, Computers and Electronics from Craiova, promotion 2008, being specialized in Software Engineering. During the years 2008-2010, he was a master student at the same faculty, from where he graduated with a Master in Distributed Systems degree. Currently, he finished the PhD program of the Doctoral Studies Institute at the Academy of Economic Studies in Bucharest, with a specialization in Economics Informatics. Main fields of interest for him are: information and communications security, distributed systems, collaborative systems, database systems, object oriented programming using Java, C++, C#.

DOI: 10.12948/issn14531305/18.4.2014.12