Security metrics to improve information security management

Igli TASHI, Solange GHERNAOUTI-HÉLIE

HEC Business School –University of Lausanne
Switzerland

Abstract

The concept of security metrics is a very important aspect for information security management. Security metrics are tools to facilitate decision making and to improve performance and accountability. The aim of information security is to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents. In that way security is not only a technical matter. In a security metrics generation perspective, organizations must take into consideration all information security dimensions including technical, organizational, human and conformity aspects in order to be competitive whilst providing stakeholders detailed information about the complete structure of the organizations' information security and risk treatment processes. This paper discusses ways to identify the right metrics to measure security preparedness and awareness within an organization.

Keywords: *Information Security, Risk assessment, Security metrics, Security management efficiency, ISO 27001 and ISO 17799 standards*

1 - Needs for security metrics

The technological explosion nowadays forces organizations to change their functioning and structures. Technology becomes the main factor for productivity growth and organizations' competitiveness and allows effective cost reductions. The use of technologies, their role and importance are increasing more and more by day.
The current hefty globalisation and de-localization phenomena should not be ignored any more. Organizations externalize their production activities more and more following a so called "company without factory" model. Thus, an organizations' communication centre becomes increasingly important as they are depending more on their information system then they did in the past. A dysfunction of such centre can paralyse all the system and could have disastrous consequences for the company at many levels (financial, reputation etc.). The risk of paralysis could be even more critical for companies whose principal asset and added value is information. A typical highly vulnerable sector for such risks is for example the services sector. Security issues within an organization must therefore be treated as a priority at top managerial level.

Under these circumstances, the top management must deal with security management as being part of their duties, besides of running the organization, which increases the complexity of decision making. Multiple strategic decisions concerning information

security have to be taken at top management level in order to assess how much resources one has to allocate, which are the risks the organization is ready and prepared to accept, which are the security needs of the organization etc. At the same time it is difficult to assess the effectiveness of organizations' security installations. For that purpose, the use of metrics to size up the information security effectiveness and efficiency are an important process for the organizations' management.

According to National Institute of Standards and Technology (NIST)[1], the security metrics' concept is outlined as a tool facilitating decision-making and improving the systems' performance for a specific organization or situation.
Security metrics can be required by laws, regulations or even by governmental administrations. For example the Federal Government of the United States requires that the security metrics must be integrated in the security programs of a government agency. Relating to this, the Clinger-Cohen Act, the Government Performance and Results Act (GPRA), the Government Paperwork Elimination Act (GPEA), and the Federal Information Security Management Act (FISMA) can be mentioned.

2 - Security metrics as a decision making tool for IT security Management

2.1 -Information Security Metrics' concept

The security metrics can be used to achieve the following goals[2]:

- To evaluate performance and to optimize protection level
- To establish a reference level about monitoring and improvement of the organizational security level, to contribute to the definition of the security level to be reached, to follow up the evaluation, validation and the optimization of the security requirements;
- To contribute to the improvement of the existing security practices and to the integration of information security within business processes;
- To contribute to the fact that technical problems should be apprehended on the managerial level;
- To justify the budgets related to the information security;
- Etc.

It is the organizations' concern to develop and collect information in order to create security metrics. That can be achieved by carrying out some measurements of the security policy implementation and assessing some results of the security services delivered according to the security measure impacts to the business processes etc.
To achieve this goal, security metrics intervene into the decision making process as shown in figure 1. The questions that have to be asked are why we need to measure and

[1] IT security metrics, Information Technology Laboratory, National Institute of Standards and Technology
[2] Adapted from " Security Metrics Guide for Information Technology Systems", NIST Special Publication 800-55

what are the things we are going to measure? These questions have to be linked with the informations' security requirements and need to give information on which way these requirements are to be performed. In consequence to that, organizations can focus on accomplishing their most critical security objectives and optimise the resources put in place.

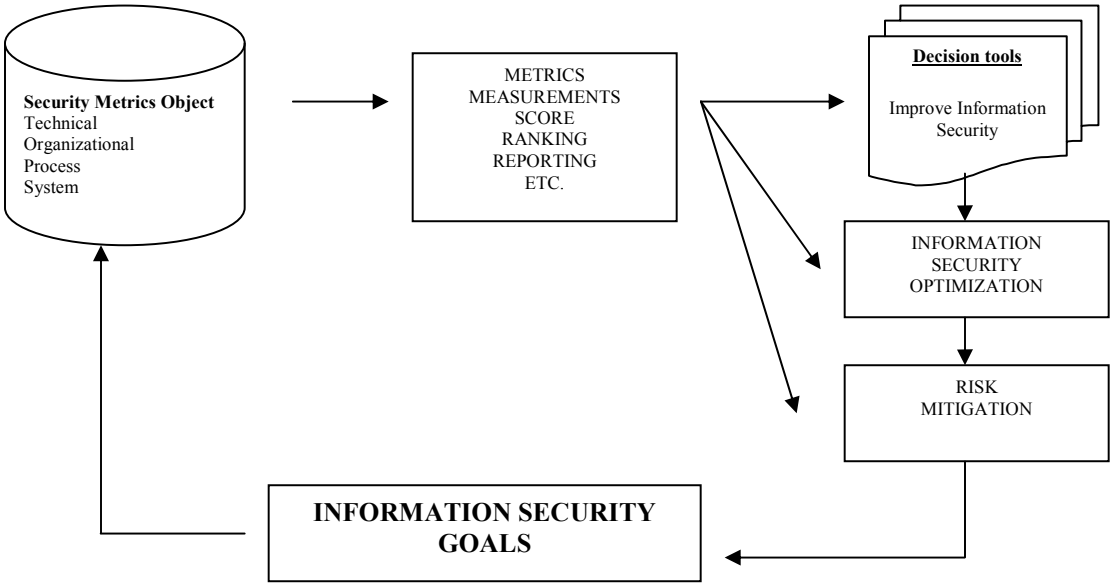

Fig. 1 : Security Metrics as management's decision-making tool

2.2 - One term, several meanings

Different interpretations or meanings are often associated to the term security metrics which can be considered as a characteristic element of a system which should be quantifiable and measurable. They have to be considered as a reference point which allows the appreciation of the systems' quality. But a controversy exists when the term "security metrics" is used. This term is very often used to describe the concepts of metric, measure, score, rating, rank or assessment. But the most important purpose for which the information security metrics are being developed is to specify if they are designated to a decision support or to a mandated reporting of information security posture.
Their variations in values reflect the dynamical character of the system. The values' analysis affords a validation of the information system conformity to a situation and to the goals to be reached.

Generally, the security metrics are classified according to the finality of their use. Thus, security metrics should be distinguished as contributing to[3]:

- risk analysis by estimating the intrusions' probability, their consequences and impacts;
- the systems' classification into classes according to the security characteristics and mechanisms;
- security strength considering the time spent to penetrate the system;
- the audit and the evaluation of the security level

The NIST SP 800-26[4] document proposes five general levels to be considered as a security metric definitions' basis, related to the information systems:

- Having security policies;
- Having detailed security procedures;
- Implementing these procedures;
- Testing the conformity and the efficiency of these procedures;
- Integrating security policies and procedures to the daily operations.

In our understanding for an efficient information security management, a meaningful security metric program has to:

- be aligned with the organizational objectives,
- be relevant to the organization's current issues,
- be quantifiable and be associated with costs.

2.3 - Information Security Metrics' advantages

The use of security metrics could bring a great number of organizational and financial advantages for the organization. It could improve the sense of responsibility with regard to the organizations' information security. Through the results obtained, organizations' management can locate the technical, operational, or managerial measures which are correctly or incorrectly implemented. These results make it possible to locate the problems and solve them. In this way, security metrics could be a useful lever to release the necessary funds for the information security functions. In addition the use of security metrics makes it possible to check and attest that the activities of the organization are in agreement with the applicable laws (compliance concept).

The security metrics measuring the performance can be classified in two groups:

1. Security metrics related to the effectiveness: To evaluate to what degree the objectives are being met;

[3] Process Approach to Information security Metrics in Finnish Industry and state Institution, Annie Sademies, 2004

[4] Security Self-Assessment Guide for Information Technology Systems, NIST Special Publication 800-26

2. Security metrics related to the efficiency: Which shows the proportionality between the objectives being reached and the results being obtained.

The use of security metrics confirms that the organization applies a proactive fail-safe attitude. These security metrics inform on the effectiveness of the processes, procedures and controls implemented into the organization.

Last but not the least, security metrics could constitute a powerful tool for the insurers dealing with Information Risk Insurances. Indeed, one of the principal matters moved forward by insurers is the absence of some shared common reference frame having an international consensus over the information system security.

2.3 - International standards' role for information security metrics and management

Security metrics are a very important management tool. They contribute to know if an information system is "in good or poor health" in order to ask the right question and have the right picture of the organizational ICT posture. Several methodologies concerning the security metrics already exist but they are focused more on the technical dimension and linked measurements rather then the way the security issues are managed. In this paper we focus on some security metrics linked to the managerial aspect of information security. So if we take into consideration that security metrics allow to take the right decision to improve information security, within their conception one must consider the managerial concerns. From this point some well recognized and largely shared methodologies and indicators concerning the management area are necessary.

International standards ISO 177799 or ISO 27001 could contribute to define the security domains to be taken into consideration to improve the information security management. Thus they could permit to specify the appropriate security metrics for the organizations. Indeed, many technical security metrics such as intrusion detection metrics, unavailability of information network etc. are largely used to specify or to state the security level of the organization. These metrics are supposed to treat the efficiency of the security tools. That way, they do not allow measurement of the global security level which is not defined only by the quality of the security tools in place. This procedure gives some punctual information which does not correlate all security elements, like the users' behaviour for example. In order to have this global vision, some "managerial metrics" are required because management quality affects the security quality. According to this statement, we can further state that if we need to improve the security level we also have to improve the information security management. This requires the use of managerial metrics in order to measure the efficiency of the current management system. Considering the fact that some international standards treating the informations' security domain already exist, we were interested to identify some parameters and measurements to be carried out in order to evaluate the security level of the organization.

The use of international standards makes it possible to speak the same security language and to better understand the concepts of security effectiveness and efficiency on today's business interactive and complex world.
After a short presentation of ISO 17799 and ISO 27001 standards, we point out the advantages that each standard brings on a security metric perspective.

3- The ISO 17799:2005 standard

3.1 - Standards' presentation

In the 90's, the representatives of some large companies like Shell, British Telecom, Marks & Spencer defined a "code of best practices" according to their experience. This document was taken up again and published by British Standard Institute (BSI). In 1995 the first BS 7799 standard appeared, under the title "Code of best practices for information security management". This document was passed to ISO to be standardized under the named ISO 17799:2000 Code of practice for information security management. Since, a new version of the ISO 17799 (BS-7799: part1) was published in 2005 (ISO 17799:2005.) This standard proposes recommendations which contribute to the information security management being destined to the persons in charge of the definition, implementation or maintenance of organizations' information security. It constitutes a common base of development of the information system security. The ISO standard defines the information security as the protection of the availability, integrity and confidentiality of the information assets as well as being in a written, spoken or digital form. That is to ensure the business continuity, the damage reduction, but also to maximize the return on investment of Information Systems. The ISO 17799 standard is an approach based on the risk management, to plan out a suitable policy, procedures and controls in order to better manage IT risks. This process is balanced between physical security, technical security, procedural security and human related security (figure 2). The assets managed by this standard are the informational assets like files, databases, records, the physical assets (servers, PC, laptops, computer hardware), software assets and the assets related to the services (informatics and communication departments, general services, power supply) etc.

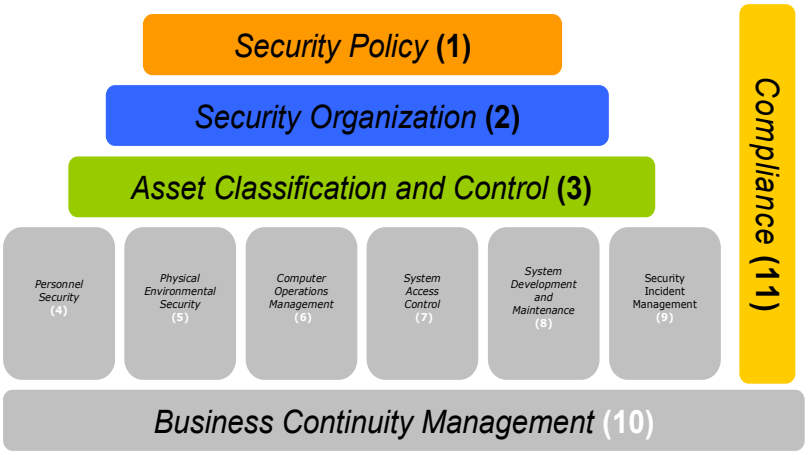

Fig. 2 : ISO 17799 :2005 chapters

The ISO 17799:2005 standard comprises 11 chapters[5] as outlined in the figure below. In the current version one more chapter, named "Security Incident Management", is added in comparison with ISO 17799:2000 standard.

3.2 - ISO 17 799 and methodologies

Aside from ISO 17799:2005 standard, several methods exist such as MEHARI, EBIOS, OCTAVE, ITIL trying to assess the IT risks. There is a method named CobiT (Control Objectify for Information and related Technology) which can also be apprehended as a security reference framework which treats several topics related to the information security management. Indeed, CobiT is an audit related best practices. CobiT (the 4th edition) helps management to establish a link between the business risks, the needs for control and the technical problems. CobiT constitutes a complete reference frame making possible to put under control the whole of information systems related operations. CobiT comprises 34 Control Objectives of System gathered in four great fields (figure 3):

1. Plan and Organise
2. Acquire and Implement
3. Deliver and Support
4. Monitor and Evaluate

The goals pursued by this method are similar to those of ISO 17799 standard. The difference is the classification between a standard and a method. Indeed, an international standard is developed by international standards organizations. By definition, international standards are suitable for universal, worldwide use and they cover large industrial and economic interests and are established in a voluntary process. On the other hand, a method is an instrument to reach effectively a precise desired result. A method

[5] ISO/IEC 17799:2005, Code de bonne pratique pour la gestion de la sécurité de l'information, www.iso.org

does not integrate the reference document concept or the consensus concept. In general, a method is the tool used to satisfy a standard.

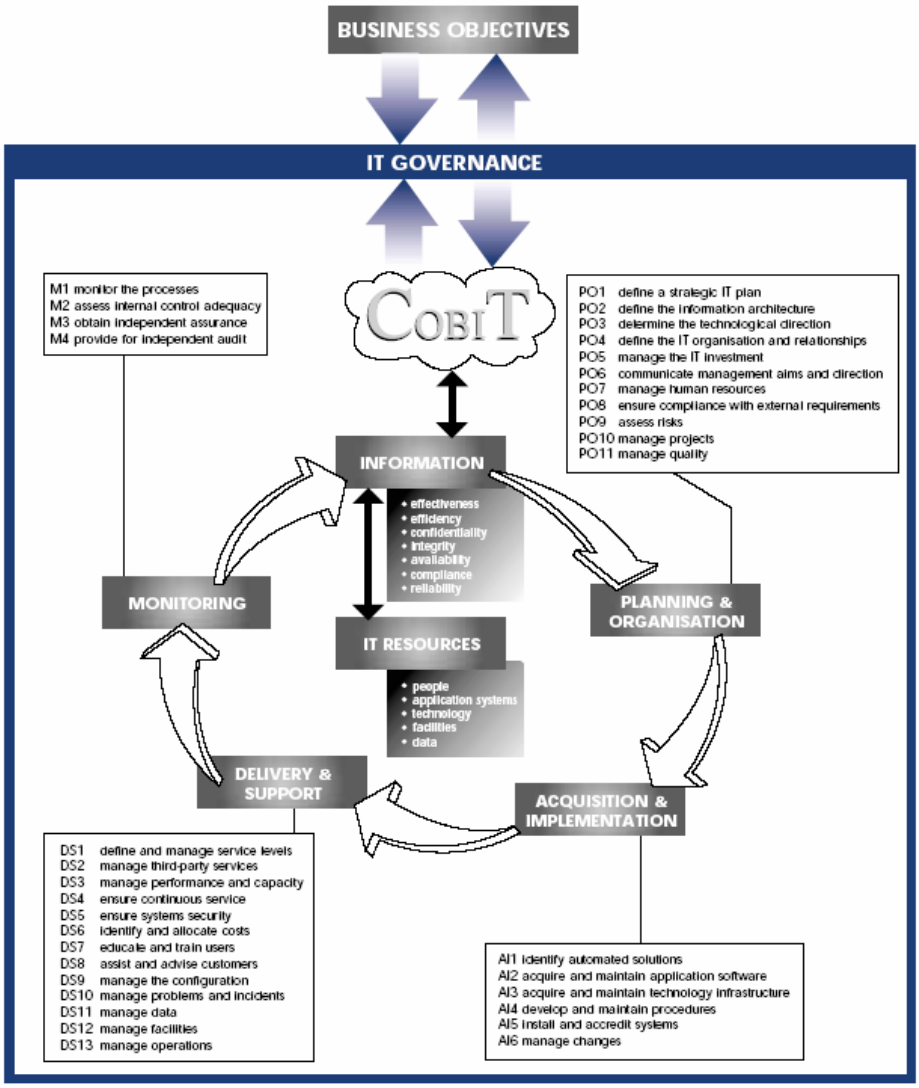

Fig. 3 : CobiT IT processes defined within the four domains

3.3 - Standards' advantages

The application of the ISO17799:2005 recommendations alerts about the principal problems concerning the information security issues and gives some recommendations about the way to better manage the information assets. It goes deeper into the corporation culture and shows that security awareness is an important component within the organization. The standards' application as well as the fact of being in conformity contributes to the information risk control and mitigation, making organizations responsible for their informational asset importance. The standard could be used to

develop procedures and solution implementations to protect these assets. Organizations will be more conscious of the measures to be taken in a total and systemic manner. Thus, a specific security reference frame could be built and organizations will be able to communicate their security strategy in an easily and comprehensible way. According to this fact, we have to focus on our intention about the security domains to be considered, in order to assess in a better way the organizational security preparedness. As it is showed on Fig. 2, ISO 17799 considers that the 11 domains represented are very important for the effectiveness/efficiency of the information security. In that way, if we consider the fact that information security is a very important component, we can imagine that we can generate measurements to state that the recommendations within the standard are reached or not. This can be made by some qualitative or quantitative metrics. For example, the standard claims that a Business Incident management is very important in an information security framework. Thus, we have to measure how many incidents occurred during a period and how many incidents are treated and communicated within the organisations' structure. We could imagine that this way of generating metrics could be applied for all the recommendations of the ISO 17799 standard. From there, the constitution of security metrics based on a largely shared methodology, knowledge and concept would be possible.

One of the greatest interests to use the ISO 17799:2005 standard resides in its international recognition, because of its ISO standard status. Originally impugned, it seems that this standard is increasingly adopted by organizations. The use of ISO 17799:2005 standard allows to simplify the use of security methods as well as communication between companies and in addition promotes the use of a common language. This allows to facilitate security comprehension and apprehension by all parties involved. In order to remain competitive in a global economy structure, organizations must be restructured by trade issues either than by country.

4 – The ISO 27001 standard and the Information Security Management System (ISMS)

4.1 Standards' presentation

The ISO 27001 standard (Information Security Management System) goes into the same direction and contains the same objectives than ISO 17799. This standard corresponds to BS 7799. ISO 27001 standard concerns all the industry and trade sectors. The difference is that ISO 27000 is a standard that anyone can be certified to, in opposition to ISO 17799 which is a standard of “best practices” concerning information security.

Developing an ISMS meeting ISO’s 27001 requirements implies having three stages (figure 4):

1. The first stage is related to the creation of a managerial framework concerning the information system. It is about fixing the directives, intentions and objectives related to information security and at the same time planning out the strategic policy which would engage the top management's responsibility.
2. The second stage is related to the risk identifications and evaluations according to the organizations' security requirements in order to define the proper managerial actions to undertake. The aim is to fix priorities to control the information security risks.
3. The last stage is related to the development of an ISMS and thus, to the selection and implementation of controls to be carried out. Indeed, once the requirements are identified, adapted controls can be selected. These controls must ensure that IT risks are assessed, mitigated and by this reduced to an acceptable level for the organization. These controls are related to policies, practices or proceedings to be followed considering the organisations' structure.

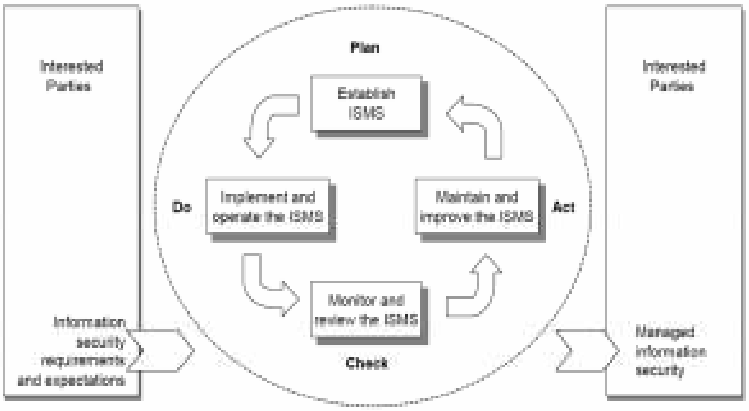

Fig. 4 :PDCA model applied to ISMS processes

ISO 27001 standard proposes and details the implementation and the documentation required for an ISMS. ISMS is the approach proposed by ISO 27001, to validate and document the existence of a managerial approach concerning the information security management, being completed by certification proceedings. An ISMS is conceived in a way to ensure that adequate and proportional security controls are selected. This standard is increasingly used by organizations as shown in figure 5:

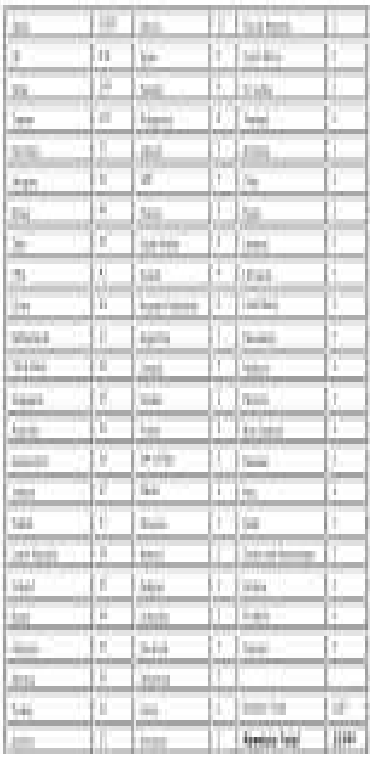

Fig. 5 : Number of certificates per country*, Source : ISMS International User Group*

4.2 - Standards' advantages

ISO 27001 standard is an international standard which provides organizations with some "best practices" in order to identify, assess and control the informational risk related to a strategic business plan and an operational environment. Obtaining a third party certificate attests that you have treated, implemented and controlled the information security. This allows the organization to be positioned in the competitive market. Amongst others, certification makes it possible to inform and consolidate the stakeholders about the way organizations' information system is protected. That can lead to increase an organizations' credibility and confidence level. Additionally, certification leads to a cost cut because certification contributes to the reduction of incidents' frequency and thus reduces costs associated with their impacts. Certification does not certify for a "security level" but for the way IT risks are managed within the organization. More specifically, ISO's 27001 certification attests that the organization has put in place some proceedings and an information security management system as well as a risk analysis system. After that, the standard certifies the relevance and the effectiveness of the implemented resources. The ISO standard within Appendix A proposes 134 controls shared out into 11 topics concerning all these aspects.

In a metric point of view the standard ISO 27001 can be considered to be a source of the variables to be used in order to measure information systems' effectiveness and

conformity. The fact of being certified ISO 27, as mentioned above, attests that the organisation has a well organised ISMS. In a metric point of view we can measure how this ISMS is implemented and which are the results. These results will show if the organisation meets the requirements or not. One of the stages of an ISMS program is the corrective actions stage. A very useful metric to be taken into consideration for the effectiveness/efficiency of the topic could be the "how many causes are identified / how many are remedied" rate. Another control to be carried out is for example the "human resources'' security management. One control is to clarify if all the employees have already signed the information security statement. A very useful metric in this respect could be to assess the percentage of "total number of employees / the number of employees that have actually signed this document".
The security metrics model can be seen as an abstraction in Henning's (2001)[6] definition, which divides IT metrics into four categories:

- Technical,
- Organisational,
- Operational
- Brainstormers', which refer to synthesis, big-picture type of metrics.

Moreover, we find the same idea in the NIST's SP 800-26 document, proposing five general levels about security metrics. Finally, thanks to the ISO 27001 standard, a structured information security management system could be conceived in the future.

5 - Conclusion

The concept of security metrics is a very important aspect for information system security. As mentioned above, security metrics are specific tools facilitating the decision making and improving the systems' performance for a specific organization or situation. To reach this goal, first of all, the objective being measured must be explicitly specified. Our goal within this paper was to measure the effectiveness of the security strategy set up within an organization. It is like a score, rating or rank regarding the IT security posture.

According to ISO 17799, the purpose of information security is to ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents.
In that way the security is not only a technical matter. Organizations must take into consideration other dimensions of information security like organizational, human and conformity. Only all these dimensions together, including the technical one, can ensure a good defence level against IT threats and risks.

As mentioned above, ISO information security standards–related gives some recommendations or controls to be implemented considering all these IT security

[6] Henning, R. (ed.) 2001. Workshop on Information Security System Scoring and Ranking. Information System Security Attribute Quantification or Ordering

dimensions. With them in mind, we can reach the main objective of measuring information security effectiveness and awareness.

In our opinion, the development of a common approach concerning security metrics allows a global information security control "from beginning to the end", independent from any great number of parties being involved.

References

- GHERNAOUTI S. (2006), Sécurité informatique et réseaux : cours et exercices corrigés, DUNOD
- Calder A. (2005), The case for ISO 27001., UK, IT Governance Publishing.
- Jones A., Ashenden D. (2005), Risk management for computer security., UK, Elsevier.
- Cohen F. (2006), IT security governance Guidebook with security program metrics., Auerbach Publications, US
- ISO/IEC 17799:2005, Code de bonne pratique pour la gestion de la sécurité de l'information, www.iso.org
- ISO/IEC 27001, Information security management system-Requirements, www.iso.org
- Kajava J., Savola R. (2005), Towards Better Information Security Management by understanding Security Metrics and Measuring Processes, cahier n°02 – 2001, University of OULU , *(Finland)*.
- NIST National Institute of Standardization and technology. (2003), Security Metrics Guide for Information Technology System , NIST , *(USA)*.
- NetSec. (2004), Using metrics to improve security, *(USA)*.
- BH Consulting. (2005), BS 7799 becomes ISO 27001, (Ireland)
- Manas-Argemi J. (2005) "Security Metrics and Measurements for IT" , , The European Journal for the Informatics Professional Vol. VI, issue No.4
- Sademies A. (2004), "Process approach to Information Security Metrics in Finnish Industry and state Institutions", VTT Publications 544, Finland
- Henning, R. (ed.) 2001. Workshop on Information Security System Scoring and Ranking. Information System Security Attribute Quantification or Ordering (Commonly but improperly known as .Security Metrics.). [Web-document].
- http://www.nist.gov
- http://www.xisec.com
- http://www.securityrisk.co.uk
- http://www.ssi.gouv.fr/
- https://www.clusif.asso.fr/
- http://www.17799.com
- http://www.27001-online.com/
- http://www.ysosecure.com/