Measuring Security

Alfonso Bilbao
Cuevavaliente Ingenieros
28760 Tres Cantos
Madrid, Spain
abilbao@cuevavaliente.com

Enrique Bilbao
Cuevavaliente Ingenieros
28760 Tres Cantos
Madrid, Spain
ebilbao@cuevavaliente.com

***Abstract*—Measuring Security is a clear need widely spread in the field of Cyber Security. It is part of the standardized risk management, such as ISO 27001, and it is an essential tool in the PDCA cycle of continuous improvement.**
On the other hand, in Physical Security environment just a few organizations are still using risk management systems oriented on continuous improvement, based on PDCA cycles, such as ISO 31000.
This may be the reason why Physical Security does not have extended experience on how to measure its performance.
Notwithstanding, Managing Security, Information Technology, Customs Relations, Production, or any other function of a company or organization should be measured.
Obviously what it is not measured cannot be evaluated. And if you cannot evaluate a function of a company, how do you know if their leaders are doing well? How do you know if you are providing appropriate resources or not? In this paper we analyze which Security aspects can be measured and how.
Several sets of parameters are proposed to be considered, in order to analyze the Security resources of an Organization:
- Effectiveness (incidents and the success of his rejection)
- Efficiency (money, people, work hours)
- Performance (equipment breakdowns attendance times, officers absenteeism, etc.)
- Evolution of the threats addressed (incidents and attempts)
- Maturity of the resources (projects planned, implemented, on operation, audited)
The existence of a methodology for measuring Security is essential in the implementation of a risk management system focused on continuous improvement.
Measuring Security is a key to propose organizational goals and generate benchmarking among different branches or at different moments.
Cuevavaliente Ingenieros has specific experience on implementing security metrics for international companies.

Keywords: Security; Metrics; ISO 31000; effectiveness; Efficiency

I. THE ISO 31000 STANDARD

The publication of the new ISO 31000:2009 Risk Management standard [dated November 13, 2009], provides an opportunity for the standardization of the Security Sector against deliberate Physical Hazards.

The importance of this event is based on the following two reasons:

- It covers the entire spectrum of the Security Risk Management (such as ISO 27001 for the computer Security)
- It is also focused on continuous improvement to the scheme Plan-Do-Check-Act, PDCA (Plan, Do, Check and React, typical of the ISO standards.

The ISO 31000 is intended to all types of businesses and organizations and, in general, to all kinds of "Securities", being very easily adaptable to Physical Security. Its implementation in a company would provide a set of procedures and regulations to guarantee among other dimensions the following:

- Having clear objectives in the Security Systems Management, oriented to business and assumed by senior management team.
- Having a specific regulatory body, harmonized with the internal regulations of the company.
- Having a Risk Analysis agreed with the General Management of the company, which directly determines the required arrangement of resources of Security (expenditure and investment Plan)
- Having a Security execution metric, in order to analyze deviations from goals and Security performance.
- Having execution analysis procedures (from the metric) which produce the subsequent decisions which have an inclination to correct possible deviations.

The implementation of ISO 31000 models will align the "Security function" (or "Security processing") of companies and organizations, with the ultimate goals of these organizations, and will also generate the methodology for continuous function improvement and measuring.

This will "standardize" security within organizations.

ISO 31000 proposes a scheme as the one in the Fig. 1 for the implementation of a Security Management System.

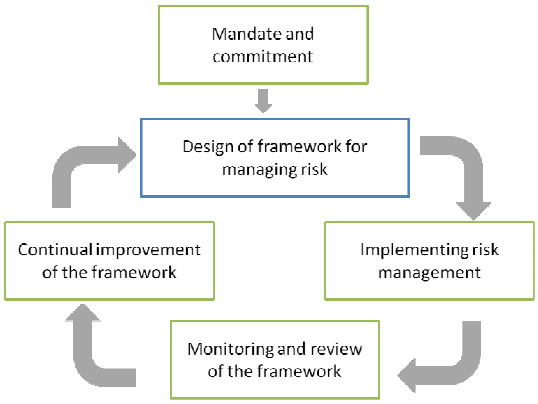

Fig. 1. ISO 31000 Security Management System proposed scheme

Each of the modules or stages is below.

A. *Mandate and Commitment*

The implementation of a Security Management System requires a strong commitment and involvement by the management in the highest level possible and so the management should develop a regulatory scheme for the gathering of the following:

- Set up a Security Policy and a Security Plan.
- Determine performance indicators for the execution of the Security Plan consistent with other indicators of organizational performance.
- Aligning Security Plan objectives with the objectives and strategies of the rest of the organization.
- Ensure the compliance of the applicable law.
- Assign auditable responsibilities at appropriate levels of the organization
- Ensure adequate provision of resources for the Security Plan.
- Communicate the benefits of the Security Plan to the Property.
- Ensure that the policy framework of the Security Plan continues to remain adequate.

Physically these provisions will result in directives or standards at the highest level of the internal rules of each entity.

B. *Design of Framework for Managing Risk*

This activity will provide a series of documents (Standards and Procedures) in which it is determined:

- The organization and its context.
- The Security Policy Security Department itself.
- The integration of Security in the rest of the processes of the organization.
- The form of control to be applied to the Security Plan.
- The resources provided for Security.
- Internal Communication and information mechanisms.
- External Communication and information mechanisms.
- Risk Analysis of assets to be protected.
- Criteria for the implementation of security measures according to the risks analyzed.

C. *Implementing Risk Management*

This phase implements what has been planned in the previous phase. To achieve this:

- Determines processes to implement.
- Distributes in Projects the available measures identified.
- Distributes Projects over periods (months, years).
- Runs Planned projects.
- Audits results.

D. *Monitoring and Review of the Framework*

For Monitoring and Reviewing the Security Plan, the following activities will be undertaken:

- Determination of performance indicators (how to measure the effectiveness of the Security Plan).
- Periodic review of the indicators with the corresponding reports on deviations.
- Periodic review of the Framework for Security Action Plan and report of their compliance with the organization's current circumstances.
- Security Incident Reports of the progress of the implementation of the Security Plan and the implementation of Security Policy in both cases.

E. *Continual improvement of the Framework*

Closing the circle of continuous process improvement is achieved by the actions of redefining the Plan to allow adequate the Security Policy, Security Plan itself and the framework of the Security Action Plan.

The frequency of these reviews must be defined in the Security Plan itself and depend on the complexity and circumstances of the organization.

II. THE METRIC IN SECURITY MANAGEMENT

The Security Management, such as Computer Technology management, Sales management, Production management, and any other function of a company or an organization either, must be measured.
As we all know, what is not measured cannot be evaluated.

And if you cannot evaluate a function of a company, how do you know if its leaders are acting correctly? How do you know if the resources provided are adequate resources or not?
An efficient Security Management scheme, such as the one just mentioned included in ISO 31000, must contain a process step focused on measurement, called Monitoring and Review (Check in the scheme Plan_Do-Check-Act) .

The key for properly accomplish monitoring and review of the framework activity is, among others, the determination of execution indicators (how to measure the effectiveness of the Security Plan).

How often Security managers have had to defend a budget in front of the Steering Committee with no arguments.
How often those responsible for Security at a corporation found lacking procedures to assess the performance of their subordinates in charge of security in different buildings or establishments.
There is no doubt that security measure is critical.
What can be measured in the Security Management?
To answer this subject we must bear in mind that the life of a Security Department runs between the development of projects (whether to implement new procedures, installation of security systems, changes in vehicle control, etc.) and the operation of existing resources (access control systems, guarding services, personal protection services, maintenance management, etc.).
Both the performance of ongoing projects and the operation itself should be measured.

Ongoing projects are easy to measure, basing metrics on accomplishing dates (project definition, implementation, commissioning and review), and budget (investment and expenses). Setting the metric for this activity is simple, and identical to the ones used in other departments of the company.

It is more difficult to establish a metric for the operation. In any case, when established, this metric is specifically designed for each organization.
Operation metric has to be designed according to two axes:

- On one hand the result should be measured: detected number of thefts, value of "shrinkage", alarms attended, recorded visitors, etc..
- On the other hand, ratios must be set to infer the effectiveness of the operation: rotation of the watchers, absenteeism, number of breakdowns, average mean time times of repairs, comparison between this and the expected Mean Time Between Failures (MTBF), mean time of credentials generation for new access control users, etc.

An example of operation metrics to be applied to a clothing store chain is proposed.

III. EXAMPLE: CLOTHING STORE CHAIN SECURITY OPERATION METRIC

This example presents a possible security metric applied to a business with medium sized shops selling clothes in different cities.
Stores are supposed to have the following security measures:

- A guard at the main door during opening time, monitoring the anti-theft system and possible incidents in the cash boxes.
- An anti-theft system consisting of RFID labels on the goods and detection antennas at the store exit.
- A CCTV system consisting of several cameras inside and a digital recorder.
- An intrusion detection system with indoor detectors and a central control room.
- A centralized system which comprises a router that connects the alarm to a Central Reception and TV images in case of alarm.

The metric to be designed will allow performance comparisons among different stores in the period of study (one year for example). It will also allow to set performance targets, to compare best performing stores to use them as an example for the others and to study the reasons for its success, etc.
The proposed parameters to be measured are divided into two main sections:

- Security results.
- Performance results.

The following steps may be suggested in order to obtain:

A. Security Results

A1.-"Shrink" Value or the difference between the actual inventory and the accounting data (K €)
A2.-Burglary incidents (number / year)
A3.-Thefts incidents (number / year)
A4.-Complaints submitted to the Police (number / year)

B. Security performance

SURVEILLANCE

B1.-Guarding Turnover (number/ year)
B2.-Guards Absenteeism (hours /year)
B3.- Inspections not carried out by the guard company compared to those agreed (number / year)
B4.- Defects found during the inspections (number / year)

INTRUSION DETECTION

B5.- False intrusion alarms (number / year)
B6.- Equipment breakdowns (number / year)
B7.-Average time to repair defect (days)

B8.- Real detections (number / year)
B9.- Undetected intrusions (number / year)

CCTV

B10.- Equipment breakdowns (number / year)
B11.- Average time to repair defect (days)

ANTI-THEFT

B12.- Real alarms (number / year)
B13.- False alarms (number / year)
B14.- Equipment breakdowns (number / year)
B15.- Average time to repair defect (days)
B16.- Undetected thefts (number / year)

Besides these indicators, ratios can be generated between them, such as:

- R1:Denounce efficacy (B8+B9+B12+B16-A4)
- R2: Total number of failures (B6+B10+B14)
- R3: False positives in anti-theft (B12/(B12+B13))
- Etc.

The use of the metrics in a graphical way, allows evaluating the stores in a simple manner.

Fig. 2. Security results metric for two different shops.

A1.-"Shrink" Value or the difference between the actual inventory and the accounting data (K €)
A2.-Burglary incidents (number / year)
A3.-Thefts incidents (number / year)
A4.-Complaints submitted to the Police (number / year)

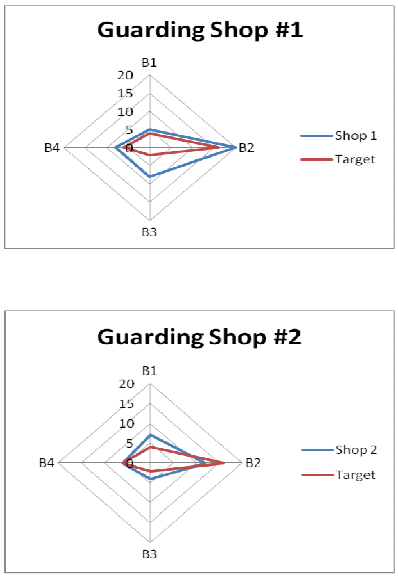

Fig. 3. Security Performance Guarding metric for two different shops.

B1.-Guarding Turnover (number/ year)
B2.-Guards Absenteeism (hours /year)
B3.- Inspections under surveillance by the company compared to those agreed (number / year)
B4.- Defects found in inspection (number / year)

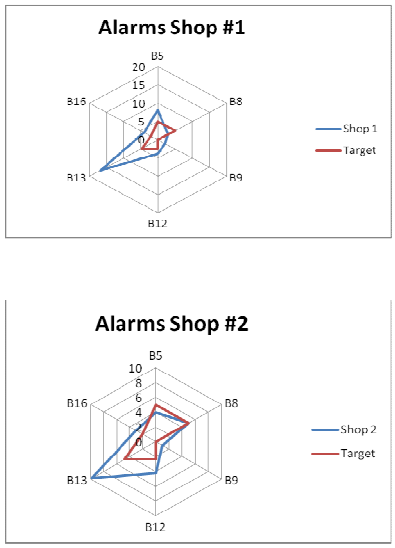

Fig. 4. Security Performance Alarms metric for two different shops

B5.- False alarms of intrusion (number / year) Intrusion Detection
B8.- Real detections (number / year) Intrusion Detection
B9.- Undetected intrusions (number / year) Intrusion Detection
B12.- Real alarms (number / year) Anti-theft
B13.- False alarms (number / year) Anti-theft
B16.- Undetected thefts (number / year) Anti-theft

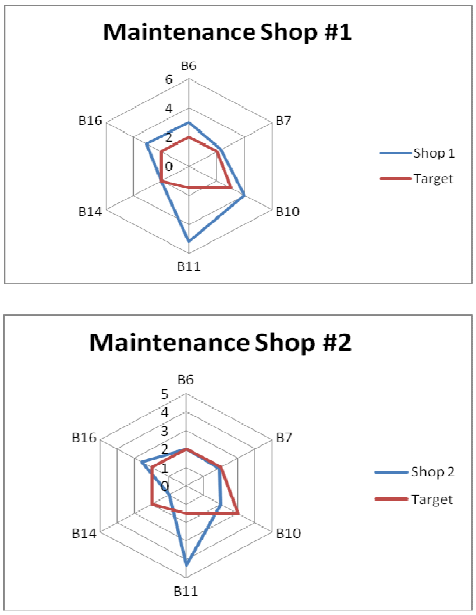

Fig. 5. Security Performance Maintenance metric for two different shops

B6.- Equipment breakdowns (number / year) Intrusion Detection
B7.-Average time to repair defect (days) Intrusion Detection
B10.- Equipment breakdowns (number / year) CCTV
B11.- Average time to repair defect (days) CCTV
B14.- Equipment breakdowns (number / year) Anti-theft
B15.- Average time to repair defect (days) Anti-theft

IV. CONCLUSION

The need for measuring elements in the performance of security is evident.

The example presented shows the simplicity of the implementation of this metric.

Professional security management must include measurement as a fundamental tool, being integrated or not in a management system for continuous improvement, as the proposed by ISO 31000.

REFERENCES

[1] G.L. Govacich, E.P.Halibozek, "Security Metrics Management", Butterworth-Heinemann, 2006

[2] "ISO 31000. Risk Mangement- Principles and Guidelines on Implementation", ISO November 2009

[3] A.Bilbao, E.Bilbao, K.Peciña, "Physical and Logical Security Management Organization Model based on ISO 31000 and ISO 27001" Proceedings ICCST, Mataró October 2011.

[4] A.Bilbao, "The Security management, it is possible to measure?" ("La gestión de la seguridad, ¿se puede medir?" in the original), Revista de Seguridad, November 2011.

[5] A.Bilbao, The Security Metrics in general and applied in the people access control" ("La Métrica en la Seguridad en general y en el control de accesos de personas en particular" in the original).JRBP, Las Palmas 2012.

[6] Richard B. Cole CPP, "Measuring Security Performance & Productivity", Asis International, 2003