Journal of Theoretical and Applied Information Technology
15 September 2012. Vol. 43 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

INFORMATION SECURITY, 4TH WAVE

[1]HICHAM ELACHGAR, [2]BRAHIM BOULAFDOUR, [3]MERYEM MAKOUDI, [4]BOUBKER REGRAGUI

[1]PhD student at the National School of Computer Science and Systems Analysis, Rabat

[2]PhD student at the Faculty of Juridical, Economic and Social, FES

[3]Professor at the Faculty of Juridical, Economic and Social, Department of Physics Laboratory LESSI

[*4]Professor at the National School of Computer Science and Systems Analysis, Rabat
E-mail: [1]elachgar@gmail.com, [2]brahim.msi@gmail.com , [3]Makoudi@yahoo.com,
[4]Boubker.regragui@gmail.com

ABSTRACT

The present paper deals with the 4th wave of the Information Security as a new approach to governance of information security. After introducing the four waves of information security, is focused on the last part which will be part of our thesis.
Based on the three waves in the development of Information Security, Information Security development is presently in its Fourth Wave. This wave reflects the development of Information Security Governance as a result of the emphasis on good Corporate Governance.
The Fourth Wave of Information Security can therefore be defined as the process of the explicit inclusion of Information Security as an integral part of good Corporate Governance, and the maturing of the concept of Information Security Governance.
We as Information Security practitioners must use this development to its optimum to ensure the security of IT systems.
In addition, following the PDCA approach (Plan, Do Check, Act), we will establish an inventory of information system with the SoM (Statement of Maturity), a risk assessment of assets, a business continuity plan to ensure a resumption of IT.

Keywords: *Security, PDCA, ISO 27002, ITIL, CObIT, Information*

1. INTRODUCTION

Applications Today, information can be viewed as a commodity, like electricity, without which many companies and organizations cannot function. However, in the interconnected world we live in, information is much more vulnerable than other commodities. While it is highly unlikely that the actions of a disgruntled teenager on another continent affect the electricity supply company, it is easy to envisage that the actions of this youth can stop the system Information from prestigious organizations.

It is therefore essential for organizations to ensure continued access to information while protecting their information assets. Many organizations will not do business without access to their information resources. However, the protection of information resources often has no direct return on investment. The security of information resources as a rule does not generate revenue for an organization.

Therefore, investors are rarely interested in how their information resources are protected. From a business perspective, the information security is not an axis of development organizations, which are more likely on the profitability of investment, which considerably slows down investment in information security.

In this regard, the information security has gone through several stages [1]:

The first wave was characterized by the reduction of information security to a technical problem left in the hand of technical experts.

The second wave was marked by the passage of information security from a technical dimension to a dimension of management by including policies and procedures.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

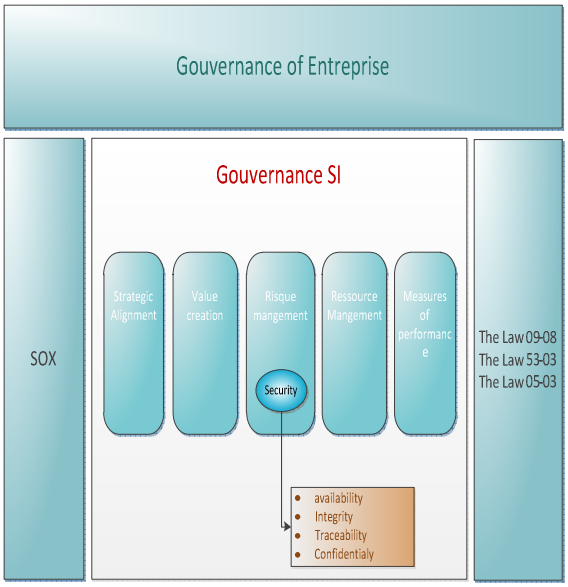
The third wave was characterized by the need to adopt some form of standardization of information security and integration of aspects of best practices, certification, and integration of culture and information security of the measurement and monitoring.

The fourth wave is the development of the Governance of Information Security. The origins of this wave are closely linked to developments made in the areas of corporate governance and especially in legal and regulatory requirements. The board felt the need to secure information systems because they started to become personally responsible for the security of their information systems [SOX, BASEL II, ACT 0908].

This paper addresses this wave, and highlights the relationship between corporate governance and the governance of information security.

2. CORPORATE GOVERNANCE AND INFORMATION SECURITY:

Several documents related to corporate governance have emerged in recent years; the importance of governance in general is now internationally established. Corporate governance is defined as " all taken responsibilities and practices implemented by a general direction in order to provide a strategic direction, ensure objectives are met, to ensure that risks are managed appropriately, and ensure that organizational resources are used responsibly. " Corporate governance makes it clear that the board of administration is responsible for ensuring information integrity of accounting and financial reporting, and compliance with laws.
Several legal and regulatory developments related to corporate governance have focused on the role and responsibility of the Board, including the Sarbanes - Oxley (SOX, 2002) which also requires putting in place a system control related to operational risks that often result in the establishment of measures to manage risks related to security of information systems. It is therefore clear that, although not directly mentioned, there is a significant relationship between corporate governance and information security. The following diagram helps illustrate the relationship with corporate governance and information security.



3. THE GOVERNANCE OF INFORMATION SECURITY : THE 4TH WAVE:

ISACA defines the governance of information security as a kind of strategic alignment, value creation, risk management, performance management and also management of resources against Requirements Company's business. It is part of the axis of risk management and top management must assure the availability, confidentiality, traceability, integrity of information, as well as compliance with laws and procedures when handling and storage of information.

From this perspective, the governance of information security aims to ensure availability, integrity, confidentiality, and traceability information (DICT) is assured.

• Availability of information: ownership of information to be accessible and usable upon demand by an authorized entity, when it needs it.

• Integrity of information: ownership of information to be accurate, complete and unaltered.

• Confidentiality of information: information ownership that information is made available or disclosed to any persons, entities or processes allowed.

• Traceability information: ownership of information to be reviewed and audited. It is

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

especially possible to track all events related to information during a certain period.

Governance of Information Security governance is reflected in the establishment of a set of structures and measures that ensure:

• The management commitment and leadership to secure information systems: this commitment is reflected in the establishment of a security policy based on risk analysis, a classification of information assets by adopting methods analysis of risk such as: MEHARI EBIOS, ISO 27005, RISK IT ...

• The adoption of standards for information security, in this case: ISO 27002, ITIL, COBIT.

• The establishment of an organization and structures in charge of information security with a clear definition of roles and responsibilities of different actors (committee information security, the security official of the information, process owners (business managers), the local correspondents of security, IT professionals, auditors, ...)

• User awareness of the issues, threats and best practices in information security. They must thus be able to support the security policy information. This awareness may relate to topics related to information security: security issues, threats and vulnerability, risk management, authorization management, password management, information classification, access control, continuity of activity, compliance, ...

• The implementation of policies, processes and procedures to secure the information system

• The introduction of technology adequate to secure the information system by setting up according to the risks and needs of firewalls, proxies, antivirus, IDS, IPS, certificates, SSO, ...

• Compliance with regulatory requirements in connection with the information security information. These regulatory requirements may concern the protection of personal data, respect for intellectual property

• The establishment of a dashboard of measurement and control of the security information to be able to supervise and control the evolution of the information security. This process necessarily requires the establishment of indicators and measures of security management. These indicators should accurately reflect the levels of security in terms of availability, confidentiality, integrity and traceability of information.

4. HOW TO ENSURE GOOD GOVERNANCE OF THE INFORMATION SECURITY:

Surf the 4th wave; it is important to go through the third wave. Indeed, the adoption of standard reference and is an interesting and rewarding step that allows to prepare for the 4th wave "Governance Information System ". The establishment of good governance of information systems should follow the Deming cycle of quality. This is the application, the area of security, of Deming in four points:

• Plan (Plan): Security is planning to move from a reactive posture to a proactive posture;

• Develop (C): Security is a set of processes to be developed following a security benchmark.

• Check (Check): Security is controlled through audits and penetration tests, and most common methods;

• Act (Act): All control activities carried out during phase "Check" are likely to highlight a number of malfunctions that need to provide for corrective actions, preventive actions and improvement actions.

Plan	P1. Commitment of top management P2. Risk Analysis P3. Measure of maturity with regard to repositories of information security P4. Development of action plans P5. Definition of indicators measuring
Do	D1. Elaboration de la politique de sécurité de l'information D2. Elaboration des procédures D3. Exécution du plan d'action
Check	C1. measure C2. Analysis of measures
Act	A1. corrective actions A2. preventive Action A3. improvement Actions

P1. Commitment of top management

Governance and management of information security within the organization agrees that senior management actively support the security policy within the organization through clear direction, a commitment to honest, allocation functions and

Journal of Theoretical and Applied Information Technology
15 September 2012. Vol. 43 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

explicit recognition of responsibilities for information security.

ISO 27001 [2] recommends that the Branch ensure that the objectives for information security are identified, meet the needs of the organization and are integrated into processes adapted.

In addition, senior management must formulate, approve and return policy information security to monitor the effectiveness of its implementation.

The formulation of clear guidelines clearly manifests its support with the initiatives taken to strengthen security.

P2. Risk Analysis

The MEHARI (harmonized method of risk analysis) for risk analysis is proposed by CLUSIF and is based on a top-down (top-down).

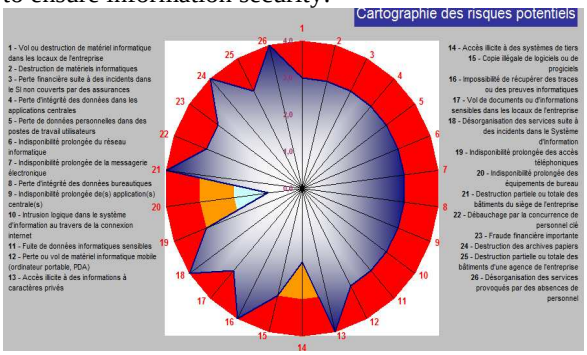
MEHARI is intended to enable risk assessment and control and security management information systems in the short, medium and long term.

The essence of this approach, allowing the risk assessment is to analyze, for a representative set of risk scenarios, the actual state of the risk level, depending on the status of security measures. This analysis will help to optimize the choice of complementary measures to be implemented.

MEHARI addresses the following areas:

1. Organization
2. Site Safety and Buildings
3. Security of premises
4. WAN between sites
5. Local Area Network
6. Network Operations
7. Architecture and Systems Security
8. Production Computer
9. Application security
10. Safety of projects and application development
11. Protecting the working environment
12. Legal and regulatory

A simplified version of MEHARI, we advocate a rosette can generate summary and prioritize actions to ensure information security:



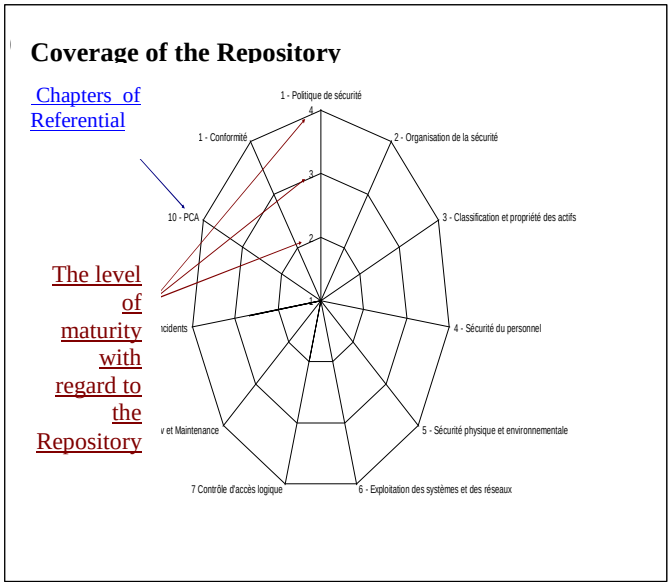
P3. Measure of maturity with regard to repositories of information security

The body of ISO 27002 identifies best practices related to information security, but does not mention the process of their implementation. Organizations can use ISO 27002 as a template to create rules and procedures regarding information security. It can be a tool to assign roles and responsibilities [3].

ISO 27002 therefore meets the needs of organizations that want to establish the objectives in terms of information security, through a series of practical recommendations, addressing both technical aspects and organization. The standard covers eleven chapters:

- Security Policy
- Security Organization
- Asset Classification and Control
- Security personnel-related
- Physical Security and Environment
- Operation and networks
- Incident Management
- Development and maintenance of systems
- Logical access control
- Business Continuity
- Compliance

Below is an example of synthesis that can be developed to measure the maturity of the security in relation to different chapters of the standard.



ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

P4. Development of action plans

Development of action plan for describing security or updating tasks for the year related to the implementation of information security within the company. This is proof of the diligence of the company to implement its security policy in practice.

- It will be used for recording the activity of the company in favor of an alignment of security on its economic goals.
- The security action plan is sequenced according to priorities, ie according to the needs of safety calculated during the risk analysis. It is a kind of operational implementation of security blueprint.

To this end, the action plan is a tool that describes [4]:

- The key priorities from these two steps in implementing security measures,
- Actions to take,
- Managers and internal resources and external support,
- The overall planning and detailed task
- Funding of this plan,
- Monitoring the implementation (progress, remains to be done... etc).

P5. Definition of indicators measuring

The use of indicators in the field of information security is a new concept. It was imposed by ISO / IEC 27001 in the MSIS without specifying how and where to use which aims to identify points of WSIS that need improvement or correction. [5]

All indicators in IS Security is a very active area of discussion. However, there are two large families of indicators ie performance indicators to verify the effectiveness of security measures and compliance indicators to monitor compliance with its specifications WSIS.

D1. Development of security policy information

Security policy ensures an acceptable level of risk for the company, by implementing a security architecture taking into account the technical, human, organizational and regulatory business. The parameters of risk analysis, when it comes to computer security are many and very different nature.

Confidentiality, integrity and availability of means of communication will be dependent on continued vigilance on the elements of:

- Physical Security: buildings, access, control, fluids, fire;
- logical security: computer backup, access, authentication, encryption ...

Knowing, of course, we are always more vulnerable by our weakest link.

Computer security is a broad concept that encompasses both application security, system security and operational safety, which also includes logical security (access management information system), physical security (site protection, fire ...) and the Communications Security Establishment.

However, the policy implementation of information security according to ISO 27001 should consider the following:

- a definition of information security, the general objectives sought and the scope chosen, and the importance of security as a necessary mechanism to share information;
- a statement of management's intentions supporting the goals and principles of information security, in accordance with the strategy and objectives of the organization;
- an approach to defining security objectives and measures, including the assessment and risk management;
- a brief explanation of policies, principles, standards and compliance requirements that are of particular importance for the organism, namely the following:
  - compliance with legal, regulatory and contractual requirements;
  - requirements in terms of training and safety awareness;
  - Management of business continuity;
  - the consequences of breaches of information security;
  - definition of general and specific responsibilities in the management of information security, addressing in particular the rise of security incidents;
  - References to documentation that will support policy and to be respected, for example policies and procedures for more detailed safety or security rules to be followed by users.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

D2. Design of procedures

In most cases, safety procedures should be supplemented by a description of the security process. These processes specify the rules by a vision of "organizational" roles and responsibilities. The bottom line is that all components of the WSIS are clearly identified. If some documents apply only partially to the WSIS, this should be stated explicitly.

This is the role of the Declaration of Applicability (SoA) which, although it is not binding outside of official certification, is a highly relevant document to build the MSIS

D3. Execution of the action plan

After determining the overall security policy of the company, it should decline the actions and measures to be taken in terms environmental, human and technical.

- Environmental Dimension:

It concerns the physical infrastructure, insurance coverage, redundancy of sites.

- Human Dimension

It involves all stakeholders of the company. Awareness of and support are the best assets to avoid malicious behavior often involuntary.

On the other hand, the Internet offers many professional services useful to businesses, but there are also on the net play multitudes of services or personal use.

The risks associated with Internet use are also a loss of productivity in the company, a saturation of the bonds, lack of confidentiality, information leakage and unauthorized downloading applications...

All these types of connections in many cases to provide important information to hackers penetrating the enterprise system.

- Technical dimension

It must be adapted and consistent with the other two dimensions. Technical solutions are plentiful, and their vendors are full of good points. Nevertheless, and because no one should be judge and jury, nothing replaces a real security audit to qualify the solution. The recipe of computer equipment must include safety testing and induce rules and procedures for verifying the security level can be maintained.

C1.Mesure

The security measures include a set of provisions to implement. These are the steps to put a good security policy.

133 measures have been defined for security information such that each was accompanied by several checkpoints to be addressed for the implementation of ISMS.

These actions occur in several areas such as asset management, physical security, compliance etc..

In MEHARI, security measures are chosen for their efficiency and robustness with respect to the severity of the disaster scenarios for the company. Four levels of severity of damage are distinguished dysfunction (4: Vital, 3: Severe, 2: Important, 1: Not significant) to develop security measures. These malfunctions can happen because of lack of confidentiality, integrity or availability of resources and data. [6]

C2. Analysis of measures

Evaluation of computer security is due to the analysis of protective measures in place to ensure information security.

These analyzes identify and take specific decisions and situation-specific, with strong involvement of the Directorate General in managing risks.

A1. Actions correctives

It comes in a “corrective” when a malfunction or a deviation is detected. It is first on the effects to correct this discrepancy or malfunction, then the causes to prevent their repetition.

A2. Preventive Action

They are launched when it detects a situation that may cause our actual or incident if nothing is done. Preventive actions are to act on the causes before the deviation occurs.

A3. Improvement Actions

Their goal is not to correct or prevent a gap, but to improve the performance of the MSIS process

5. CONCLUSION :

The concept of SSI is a set of methods, techniques and tools responsible for protecting the resources of a computer system to ensure service availability, confidentiality and integrity of information.

Security of information systems (IMS) is emerging as a critical component of protecting the company in its own interests and those related to external issues.

Given the risks involved and the functional and organizational context specific to the organization, it should identify what needs to be protected, to quantify the corresponding issue, formulate security goals and to identify, to arbitrate and implement appropriate countermeasures to correct level is maintained.

In general, the safety of SI has several objectives. Safety, then, must protect information such as company assets against data loss, disclosure or

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

alteration to ensure continuity of business operations. In addition, IS security preserves the image of the company and trust other.

6. REFERENCES:

[1] Basie Von Solms, Information Sécurity- the fourth Wave, computers & security 25 (2006) 165-166.

[2] Technologies de l'information —Techniques de sécurité — Code de bonne pratique pour la gestion de la sécurité de l'information, Première édition, 2005, page 8.

[3] Abdelhaq ELBEKKALI, Eric Lachapelle, René ST-GERMAIN, Gouvernance, audit et sécurité des TI, édition CCH, Québec, 2008, page 336.

[4] http://www.ssi-conseil.com/content/view/124/159/

[5] Thierry BOILEAU, Mise en oeuvre de la SSI (Sécurité du Système d'information) de SUSS MicroOptics par l'approche processus ISO/CEI 2700, page 43

[6] Michel KAMEL, Patrons organisationnels et techniques pour la sécurisation des Organisations Virtuelles.