7

Information Security Management Accounting

Diego Abbo
Candidate School of Systems Enginireering SSE- University of Reading (UK), Italy

1. Introduction

Increased computer interconnectivity and the popularity of Internet are offering organizations of all types unprecedented opportunities to improve operations by reducing paper processing, cutting costs, and sharing information. However, the success of many of these efforts depends, in part, of an organization' ability to protect the integrity, confidentiality of the data and systems it relies on.

Many people seem to be looking for a silver bullet when it comes to information security. They often hope that buying the latest tool or piece of technology will solve their problems. Few organisations stop to evaluate what they are actually trying to protect (and why) from an organizational perspective before selecting solutions. In the field of information security the security issues tend to be complex and are rarely solved simply by applying a piece of technology.

Furthermore the growing of interdependency of the complex integrated information systems will continue and accelerate and more technologies are integrated to deliver rich services. Today there is no way to model, understand, monitor and manage the risks presented by the growth of these systems. That also means that the investments in information security can't have the appropriate accuracy and follow the common principle of redundancy increasing the non-productive costs of the businesses and/or services that are supporting by the above mentioned systems.

On the other hand the failure of information security during the past decade are nothing short of spectacular. The inability of organisations to prevent increasingly dramatic compromises has led to huge financial losses, produced a great deal of embarrassment, and put every sector of the global economy at risk. Despite increasingly draconian legal, commercial, and regulatory activity, the losses continue to mount, national interests are still at risk, and "information crimes" proliferate unabated.

Security is a delicate matter. It is one of the important elements in modern communications today and has many implications on modern life. In order to manage the complexity of this subject it is essential to define the scope of the global research that should focus the protection of the information which definition is the collection of facts and can take many forms (text, numbers, images, audio and video clips).

The core tenets of information protection are confidentiality, integrity and availability, (also defined the CIA triangle) and the perspective of information security is to reduce both the

number of events that are causing information security breaches and the range of damages that are related to the aforementioned breach events. The research field must focus the frame that get under control the information that should be protected. In general terms we can assume that the information is moving, in a delivering system, from a point of production to a point of utilization, and a delivering system can be considered a multiple progressive segments of points of departure and points of arrivals for the information in accordance with the logical atomism.

Logical atomism is a philosophical belief that originated in the early 20th century with the development of analytic philosophy. The theory holds that the world consists of ultimate logical "facts" (or "atoms") that cannot be broken down any further.

The information is produced (processed) in one physical site, stored in the same or in another site and communicate through a physical meaning to the site of utilization. All the three entities (production, communication and utilization) exploit instrumental items as facilities that are hosting pertinent devices, hardware, software, operation systems, applicative programs, files, physical meaning of communication (internal and external network) and are linked to the human factors as operational management policy, training, working activities and the end purpose of the delivered information. The delivering systems have information end users that exploit it for a specific aim. Information and all the instrumental items that are components of a delivering system need specific dedicated interdepartmental protections in order to reduce the possibility of information breaches.

Therefore the field of application for this research is individuated in:

- The physical outer edge that contain all the instrumental items for producing, communicating and utilizing the information, the running of the associate information delivering system and its security architecture;
- The state of art of security engineering and management;
- The risk of breaches in the CIA triangle and in which way those breaches are influencing/damaging the purpose of the information end user;
- The set of methodology to individuate pertinent and useful metrics and its validation.

In accordance with the definition of security: “the protection of resources from damage and the protection of data against accidental or intentional disclosure to unauthorized persons or unauthorized modifications or destruction”, the research field should be inclusive of the security analysis of all the physical and digital information dimension, the purpose that is sparking off the production, the delivering and the end user information exploitation; furthermore the negotiating power with the threat and the consequences for the end user information purpose of the different kind of breaches.

The actual state of art should deal with four problems that are the addressee of information security research.

The first research problem consists in establishing the appropriate information security metrics to be exploit by those who have the control of the information. Metrics is a term used to denote a measure based on a reference and involves at least two points, the measure and the reference. Security in its most basic meaning is the protection from or absence of danger. Literally, security metrics should tell us about the state or degree of safety relative to a reference point and what to do to avoid danger. Contemporary security metrics by and

large fail to do so. They tell us little about the actual degree of "safety" of our system processes, much less about the organization as a whole. They say little about the appropriate course of action, and they are typically not specific for the needs of the recipient.

Security metrics are not well developed outside of a narrow range of IT- centric measures. While these measures may be useful for managing specific technologies such as patch management or server hardening, they are little use in "managing" overall security. There is little to guide the direction of a security program or provide the basis for making decisions.

Indeed, Andrew Jaquith of the Yankee Group expressed it well at the Metricon 1 metrics conference in 2006 during a keynote speech :

"Security is one of the few areas of management that does not possess a well understood canon of techniques for measurement. In logistics, for example, metrics like "freight cost per mile" and "inventory warehouse turns" help operators understand how efficiently trucking fleets and warehouse run. In finance, "value at risk" techniques calculate the amount of money a firm could lose on a given day based on historical pricing volatilities. By contrast, in security there is exactly nothing. No consensus on key indicators exists."

Considering any system that is delivering information from point A (where physically the information is produced or stored) to point B (final information end user) trough a range of A* intermediate points (where A* can range from 0 to ∞) the resolution of the first problem wants to introduce and validate as a baseline tool for security analysis, the following metrics:

- The measure of the functional cost of the implemented security safeguards all along the course of information ;
- The forejudged calculus of probability of breaches (complementary to the estimate percentage rate of security performances) linked to a given functional cost;
- The individuation of the pertinent domains. The domain is a logical entity through which is analyzed the tri-mission situation (e.g. Legal domain, Architectural framework domain, Governance domain and so on). The domains represent both a point of view of a functional perspective and an organizational filter of a dedicated analysis.
- The rate of information system burdening, in terms of loss of effectiveness for the end user purposes, due to security implemented safeguards.

The second research problem looks for the identification of appropriate security indicators that can be used to link the metrics of a security engineered system (first problem metrics) to mathematical indicators; those are representatives of the security of system independently of the technology employed and can also be a baseline of comparison with other systems or interconnected systems. The indicators can be seen as the negotiation power that is in force between the protection of the purpose of an information system and the possible threats. To create an array of security indicators it is both a mean of measuring the operational efficiency of information security and a tool to create regulatory standards for security.

The third research problem is related to the risk analysis. At the moment there is a consolidated literature that shows the way to identify, evaluate, estimate and treat the risk based on empirical methods. However that literature seems to be inappropriate for the information systems overall when they are interconnected with different security standards and the information is becoming under the control of different entities. The solution can be

individuated by considering the risk analysis with the existing methods and correlating it directly to the purpose of the information end user.

The fourth research problem consists in the evaluation of return of investment (ROI) for information security implementation.

2. Information security

The analysis of the actual state of art engages the general definition of security: (Abbo, Sun, Feb 2009 pp 195 – 200) "Security is a function of the interaction of its components: Asset (A), Protector (P) and Threat (T) in a given Situation. These can be represented in the equation:

$$S = f(A;P,T)\ Si.$$

This logical formula is the inspiring baseline for the whole research from Manunta (2000, p. 20) who states that security is the contrived condition of an Asset. It is created and maintained by a Protector in antagonism with a reacting counterpart (Threat), in a given Situation It aims to protect Asset from unacceptable damage.

For the three actors we can give the following definitions:

Asset: Any person, facility, material, information or activity that has a positive value to an owner - (Tipton F. H. – Henry K. 2007 - p. 789 -)
Protector: A person, an organization or a thing that makes sure that something or somebody is not harmed, injured, damaged etc; (OXFORD Dictionary)
Threat Any circumstance or event with potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service. Threat is the broadest category in a classification, becoming more specific as it moves through vulnerability, exploit, and attack - (Slade R. 2006 -)

The mere presence of interaction among all three actors (A, P, T) only means that a security context is present as some ongoing processes amongst actors. Further analysis shows that Figure 1 represents a security problem, which has still to be solved.

This definition is the preamble for further related research defined "**theory of sets for security situations** with the application of Venn diagrams.

Venn diagrams or set diagrams are diagrams that show all possible logical relations between a finite collection of sets (aggregation of things) They are used to teach elementary set theory, as well as illustrate simple set relationships in probability, logic, statistics, linguistics and computer science.

The importance of an asset to an organization does not simply depend on the monetary cost of the asset, but rather is based on the value of the asset to the organization (Rogers B.B., p. 75) . Before a consequence of loss of an asset can be reasonably evaluated, the organization itself must be thoroughly understood, which is the purpose of an infrastructure characterization. The infrastructure characterization seeks to gain an appreciation of this organizational environmental and to establish designs constraints under which the security system must operate. An infrastructure characterization consists of defining the critical missions and goals of the organisation, the infrastructure that is necessary to accomplish the mission, the legal, regulatory, safety and corporate framework, and the vulnerabilities that the organisation faces.

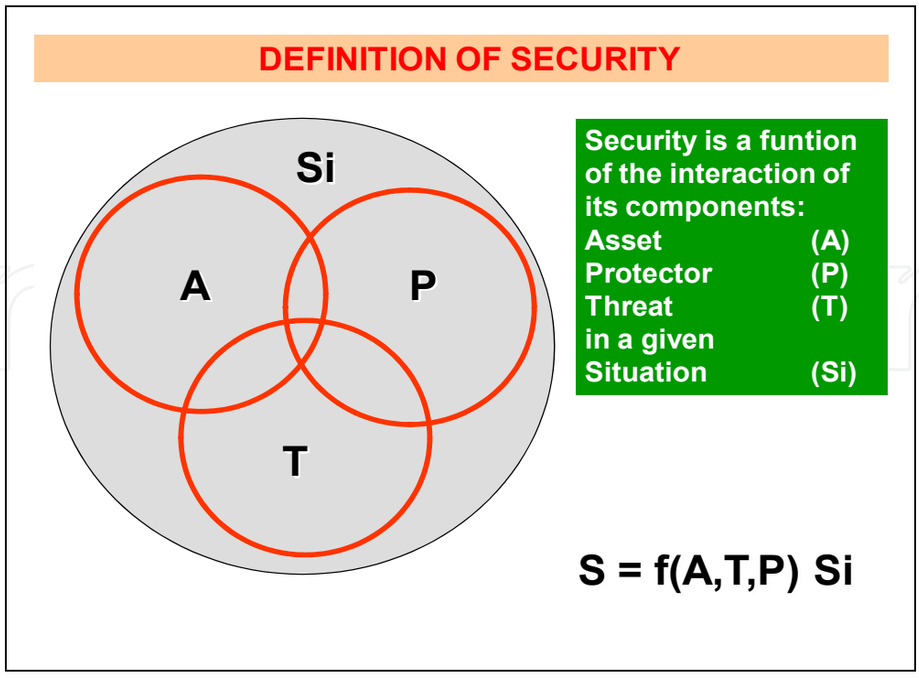


Fig. 1. Definition of Security with the application of set diagrams.

The Assets of information security issues usually include three to five elements. Examples of major security categories include confidentiality, privacy, integrity, authentication, authorization, and non repudiation. The E-Government Act of 2002, section 3542 (B), defines integrity, confidentiality, and availability attributes or security (Barker C. W. p.308):

Availability: The property of ensuring timely and reliable access to and use of information . Availability is the principle that information is accessible when needed. The two primary area affecting the availability of system are denial of service due to the lack of adequate security controls and loss of service due to disaster, such an earthquake, tornado, blackout, hurricane, fire, flood and so forth. In either case, the end user does not have access to information needed to perform his or her job duties. The criticality of the system to the user and its importance to the survival of the organization will determine how significant the impact of the extended downtime becomes.

Integrity: Guarding against improper information modification or destruction, which includes ensuring information non repudiation and authenticity.

Integrity is the principle that information should be protected from intentional, unauthorized, or accidental changes. Information stored within the files, databases, systems, and networks must be able to be relied upon to accurately process transactions and provide accurate information for business decision making. Controls are put in place to ensure that information is modified through accepted practices. Management controls such as the segregation of duties, specification of the systems development life cycle with approval checkpoints, and implementation of testing practises assist in providing information integrity. Well-formed transactions and security of updated programs provide consistent methods of applying changes to systems. Limiting update access to those individuals with a need to access limits the exposure to intentional and unintentional modification.

Confidentiality: Preservation of authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

Confidentiality is the principle that only authorized individuals, processes, or systems should have access to information on a need-to-know basis. In recent years, much press has been dedicated to the privacy of information and the need to protect it from individuals, who may be able to commit crimes by viewing the information. Identity theft is the act of assuming one's identity through knowledge of confidential information obtained from various sources. Information must be classified to determine the level of confidentiality required, or who should have access to the information (public, internal use only, or confidential). Identification, authentication, and authorization through access controls are practises that support maintaining the confidentiality of information. Encryption information also supports confidentiality by limiting the usability of the information in the event it is viewed while still encrypted. Unauthorized users should be prevented access to the information, and monitoring controls should be implemented to detect and respond per organizational policies to unauthorized attempts. Authorized users of information also represent a risk, as they may have ill intentions by accessing the information for personal knowledge, personal monetary gain, or to support improper disclosures.

The three attributes or the three pillars are also known as C.I.A triangle and are considered as classes of dimensions considering the Committee on National Security System (CNSS) model (Whitman p.5).

This security model, also known as the Mc Cumber Cube after its developer, John Mc Cumber, is rapidly becoming the standard for many aspects of the security information Systems (see Figure 2).

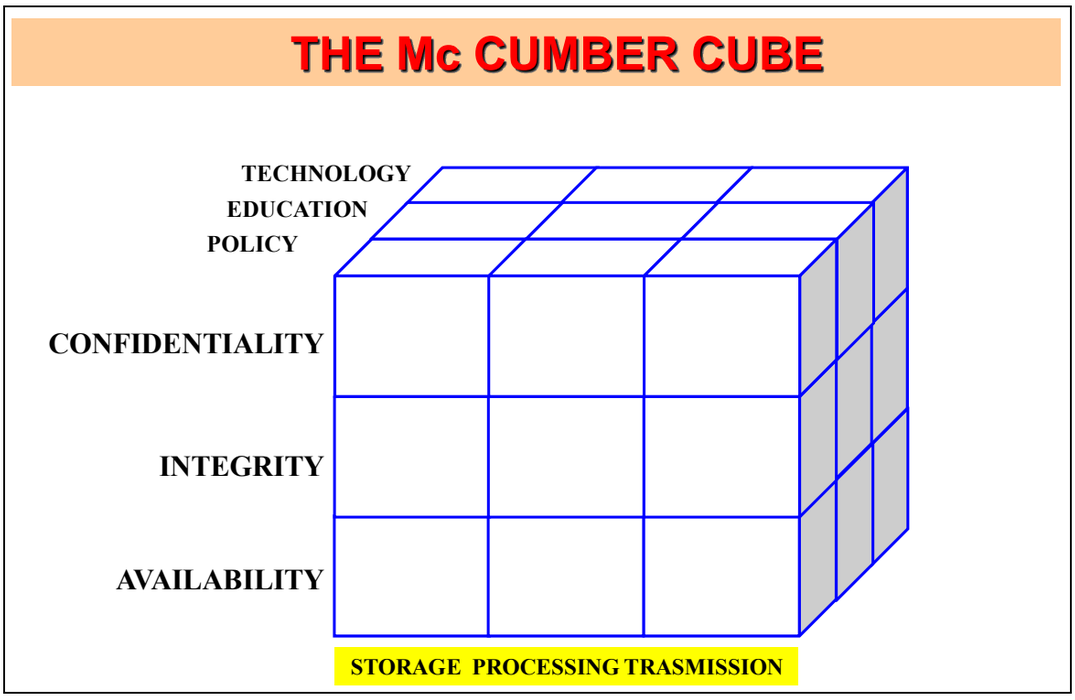


Fig. 2. The Mc Cumber cube is a model recognized by the Committee on National Security System (CNSS).

If we extend the relationship among the three dimensions represented by each axes shown in figure, we end up with a 3x3x3 cube with 27 cells. Each cell represents an area of intersection among these three dimensions that must be addressed to secure information system.

When using this model to design or review any information security program, we must make sure that each of the 27 cells is properly addressed by each of the three communities of interest. For example, the cell representing the intersection between the technology, integrity, and storage areas is expected to include controls or safeguards addressing the use of technology, to protect the integrity, of information while in storage.

While this model covers the three dimensions of information security, it omits any discussion of detailed guidelines and policies that direct the implementation of controls. However this system is very good if reused for the calculation of percentage of the single resource employed in the information security in order to define the amount of the investment.

However, in a given Situation, the ICT security is regarded as layered systems. A layered security needs to be incorporated for any assessment and evaluation process by ensuring the multiple facets of a customer's information security profile are addressed. There have been hundreds of interpretations of layered security but everyone agrees on some core areas to be addressed: network perimeter protection, internal network protection, intrusion monitoring and prevention, host and server configuration, malicious code protection, incident response capabilities, security policies and procedures, employee awareness and training, physical security and monitoring. *These areas are key points of failure within the information security architecture at many organizations"* (Rogers R., pp 5-6).

The issue is something born with the humankind's security perception, since the primordial communities, fully shown by physical layers of defensive concentricity in most archaeological evidences.

Any pertinent situation is seen by the information professional as a set of 10 organizational domains as follows (Tipton F. H. – Henry K pp. xvi-xvii):

a. **Information Security and Risk Management**: Addresses the framework and policies, concepts, principles, structures, and standard used to establish criteria for the protection of information assets, to inculcate holistically the criteria and to assess the effectiveness of that protection. It includes issues of governance, organizational behaviour, ethics, and awareness. This domain also addresses risk assessment and risk management.
b. **Access control**. The collection of mechanisms and procedures that permits managers of a system to exercise a directing or restraining influence over the behaviour, use and content of a systems.
c. **Cryptography.** Addresses the principles, means, and methods of disguising information to ensure integrity, confidentiality, and authenticity in transit and in storage.
d. **Physical (environmental) Security**. Addresses the common physical and procedural risks that may exists in the environment in which an information system is managed.
e. **Security architecture and design**. Addresses the high level and detailed processes, concepts, principles, structures, and standards to define, design, implement, monitor, and secure/assure operating systems, applications, equipment, and networks. It

addresses the technical security policies of the organisation, as well as the implementation and enforcement of those policies.

f. **Business continuity and disaster recovery planning.** Addresses the preparation, processes, and practice required to ensure the preservation of the business in the face of major disruptions to normal business operations.

g. **Telecommunications and network security.** Encompasses the structures, transmission methods, transport formats, and security measures used to provide integrity, availability, and confidentiality for transmissions over private and public communications network and media.

h. **Application security**. Refers to the controls that are included within and applied to system and application software. Application software includes agents, applets, operating systems, databases, data warehouses, knowledge-based systems etc. These may be used in distributed or centralized environment.

i. **Operations security**. Addresses the protection and control of data processing resources in both centralized (data centre) and distributed (client/server) environment.

j. **Legal, regulations, compliance, and investigations**. Addresses general computer crime legislation and regulations, the investigative measures and techniques that can be used to determine if an incident has occurred, and the gathering analysis, and management of evidence if it exists.

For the actual state has defined 13 domains as exhaustive of cloud computing pertinent situation (CSA Guidance 2009):

Domain 1: Cloud Computing Architectural Framework
Domain 2: Governance and Enterprise Risk Management
Domain 3: Legal and Electronic Discovery
Domain 4: Compliance and Audit
Domain 5: Information Lifecycle Management
Domain 6: Portability and Interoperability
Domain 7: Traditional Security, Business Continuity and Disaster Recovery
Domain 8: Data Centre Operations
Domain 9: Incident Response, Notification, and Remediation
Domain 10: Application Security
Domain 11: Encryption and Key Management
Domain 12: Identity and Access Management
Domain 13: Virtualization

The key issues are that the Situation of previous Manunta's formula [S = f(A;P,T) Si] can be viewed, in the information security environment, as a set of well defined interdependent domains each one with its organizational and operational autonomy and protection.

In addition each domain concurs with its own security share to the general protection and any security breach to a single domain reflects consequences to the breached domain and/or to other domains and/or to the general business. Furthermore a more appropriate keyword is in " security of information infrastructure" than "information security" with the following definition:

Information infrastructure. It is the satellite, terrestrial, and wireless communication system that deliver contents to homes, businesses and other public and private institutions.

It is the information content that flows over the infrastructure whether in the form of databases, the written word, a film, a piece of music, a sound recording, a picture or computer software.(Hyperdictionary).

One of the sensitive issue regarding the information infrastructure security is its measurability that means "security metrics". Security metrics are not well developed outside of a narrow range of IT –centric measures. (Brotby W. C - 2009 – pp. 13,14)

While these measures may be useful for managing specific technologies such as patch management or server hardening, they are of little use in managing overall security.

3. The risk perception

The risk is a word that admirably serves the forensic needs of new global culture and its calculation is deeply entrenched in science and manufacturing and as a theoretical base for decision making (Douglas pp 22-23).

Generally speaking Risks are generally classified as "speculative" (the difference between loss or gain, for example, the risk in gambling) and "pure risk", a loss or no loss situation, to which insurance generally applies (Broder p.630).

According to common understanding relating to the information infrastructure the risk focused assets are usually identified as the availability, confidentiality and/or privacy, integrity, authentication and no-repudiation. The risk analysis is tailored on the traditional definition of risk, according to the ISO/IEC (2002, p 2), that states "*combination of the probability of an event and its consequences, but the term risk is generally used only when there is at least the possibility of negative consequences.*"

This is defined Probabilistic Risk Assessment -PRA- (Brotby W. C p.205-). The PRA has emerged as increasingly popular analysis tool especially during last decade. PRA is a systematic and comprehensive methodology to evaluate risks associated with every life-cycle aspect of a complex engineered technological entity from concept definition, through design, construction, and operation, and up to removal from service.

Risk is defined as a feasible detrimental outcome of an activity or action subject to hazards. In PRA risk is characterized: the magnitude (or severity) of the adverse consequence(s) that can potentially result from the given activity or action, and the likelihood of occurrence of the given adverse consequence(s). If the measure of consequence severity is the number of people that can be potentially injured or killed, risk assessment becomes a powerful analytical too assess safety performances.

If the severity of the consequence(s) and their likelihood of occurrence are both expresses qualitatively (e.g. through words like high, medium, or low) the risk assessment is called qualitative risk assessment. In a quantitative risk assessment or a probabilistic risk assessment, consequences are expressed numerically (e.g. the number of people potentially hurt or killed) and their likelihoods of occurrence are expressed as probabilities or frequencies (i.e. the number of occurrences or the probability of occurrence per unit time).

In security applications, the probability of occurrence (P_O) is given by:

$$P_O = P_A (1 - P_E)$$

Where P_A is the probability of an attack and P_E is the probability of effectiveness of the security system (Rogers B.B., p. 76).

Organizations have the option of performing a risk assessment in one or two ways: qualitatively or quantitatively (Abbo, Sun - May 2009 pp 342 -346).

Qualitative risk assessment produce valid results that are descriptive versus measurable (Tipton F. H. – Henry K p. 56).

A qualitative risk assessment is typically conducted when:

- The risk assessors available for the organization have limited expertise in quantitative risk assessment;
- The timeframe to complete the risk assessment is short;
- The organization does not a significant amount of data readily available that can assist with the risk assessment.

The quantitative risk assessment is used by an organization when it becomes more sophisticated in data collection and retention and staff become more experienced in conducting risk assessment.

The hallmark of a quantitative risk assessment is the numeric nature of analysis. Frequency, probability, impact, countermeasures effectiveness, and other aspects of the risk assessment have a discrete mathematical value in pure quantitative analysis.

The risk is associated to a negative event and to the fact that for any negative event, normally, we have pure damages (the costs of the pure loss) resilience damages (the costs of reset) and consequential damages (can be the loss of image, business activity or a step of the threat to pursue other more harmful aims) (Innamorati, pp.61-62 -- my translation).

However if we consider the speculative risk it should be considered also the "positive consequences" in accordance with the concept widely accepted in the business world of no risk no return (LAM pp. 4-5).

The division of risk are limited to three common categories:

Personal (having to do with people assets);
Property (having to do with material assets)
Liability (having to do with legalities that could affect both of the previous categories, such as errors and omissions liability).

Finally it should be taken into consideration the environment in which risk management is situated (Jones, Ashenden p 244):

" Figure 3 depicts the environment in which risk management is situated. At the bottom of the diagram is the concept of trustworthiness (the trust is the predisposition to expose oneself to a security risk). In turn, this has a direct relationship to governance processes in an organization, and this influences an organization's ability to demonstrate compliance.

However should be point out that risk identification and risk estimation is both human and social activity (Tsohou A., Karyda M., Kokolakis S., Kiountouzis p.202). Different people (end –users, stakeholders, etc) or from they have been told by friends. Many factors may influence the way risk is perceived; some of them include the familiarity with the source or danger, the ability to control the situation and dreadfulness of the results.

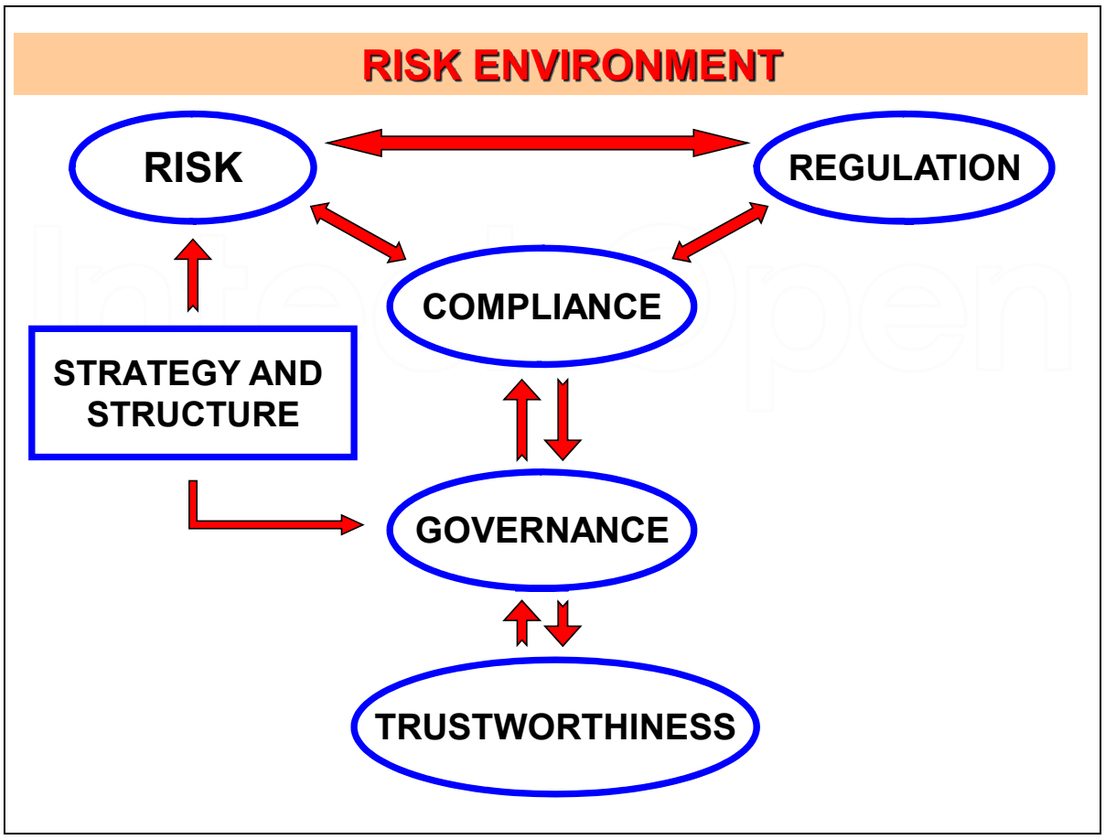


Fig. 3. The risk environment actors.

Therefore, people's ranking of threats may not coincide with that IS security professionals. In essence, much of the people's knowledge of the world comes from perceived stimulus-signs, signal and images.

4. The actual risk management approach

The top edge of security management is represented by the International Standard that adopts the "Plan–Do- Check–Act" (PDCA) model which is applied to structure all Information Security Management Systems (ISMS) process (ISO/IEC 27001 p. v–vi).

The adoption of PDCA model will also reflect the principle the principles governing the security of information systems and networks. This is a robust model for implementing the principle of those guidelines governing risk assessment, security design and implementation, security management and reassessment.

Risk management as define by "random house dictionary" as "the technique or profession of assessing, minimizing, and preventing accidental loss to a business, as "through the use of insurance, safety measures etc" (Tipton F. H. – Henry K p. 56):

A systematic approach to information security risk management is necessary to identify organizational needs regarding information security requirements and to create an effective information security management system – ISMS - (ISO/IEC, 27005 p.3-6).

This approach should be suitable for the organization's environment, and in particular should be aligned with overall enterprise risk management. Security efforts should address risks in an effective and timely manner where and when they are needed. Information security risk management should be an integral part of all information security management activities and should be applied both to implementation and the ongoing operation of an ISMS.

Information security risk management should be a continual process.

The process should establish the context, assess the risks and treat the risks using a risk treatment plan to implement the recommendations and decisions.

Risk management analyses what can happen and what possible consequence can be, before deciding what should be done and when, to reduce the risk to an acceptable level. Information security risk management should contribute to the following:

- Risks being identified
- Risks being assessed in terms of their consequences to the business and the likelihood of their occurrence
- The likelihood and consequences of these risks being communicate and understood
- Priority order for risk treatment being established
- Priority for actions to reduce risks occurring
- Stakeholders being involved when risk management decisions are made and kept informed of the risk management status
- Effectiveness of risk treatment monitoring
- Risks and the risk management process being monitored and reviewed regularly
- Information being captured to improve the risk management approach
- Managers and staff being educated about the risks and the actions to mitigate them

The information security risk management process can be applied to the organization as a whole, any discrete part of the organization (e.g. a department, a physical location, a service) any information system, existing or planned or particular aspects of control (e.g. business continuity planning).

The information security risk management process consists of context establishment, risk assessment, risk treatment, risk acceptance, risk communication and risk monitoring and review.

The level of risk is estimated on the basis of likelihood of an incident scenario, mapped against the estimated negative impact. The likelihood of an incident scenario is given by a threat exploiting vulnerability with a given likelihood.

The following shows the risk level as a function of the business impact and likelihood of the incident scenario. The resulting risk is measured on a scale 0 to 8 that can be evaluated against risk acceptance criteria. This risk scale could also be mapped to a simple overall risk rating according to the matrix in table 1 (CSA 2009, p. 21):

- Low risk: 0-2;
- Medium risk 3-5;
- High risk 6-8

Likelihood of incident scenario / Business impact	Very Low Very Unlikely	Low Unlikely	Medium Possible	High Likely	Very High Frequent
Very Low	**0**	**1**	**2**	**3**	**4**
Low	**1**	**2**	**3**	**4**	**5**
Medium	**2**	**3**	**5**	**5**	**6**
High	**3**	**4**	**5**	**6**	**7**
Very High	**4**	**5**	**6**	**7**	**8**

Table 1. Estimation of risk levels based on ISO/IEC 27005: 2008.

The subsequent management of risk is facing three basic options (Broder p. 641).

- The risk can be avoided, eliminated, or reduced to manageable proportions;
- The risk can be assumed or retained;
- The risk can be transferred to a third party. The transfer to a third party generally implies transfer of liability to an insurance carrier.

The consequent step of risk management is its reduction within levels of acceptance introducing safeguards that reduce the rate of the product probability by consequences, where both the terms are included under an ordered category as it is shown in figure 4.

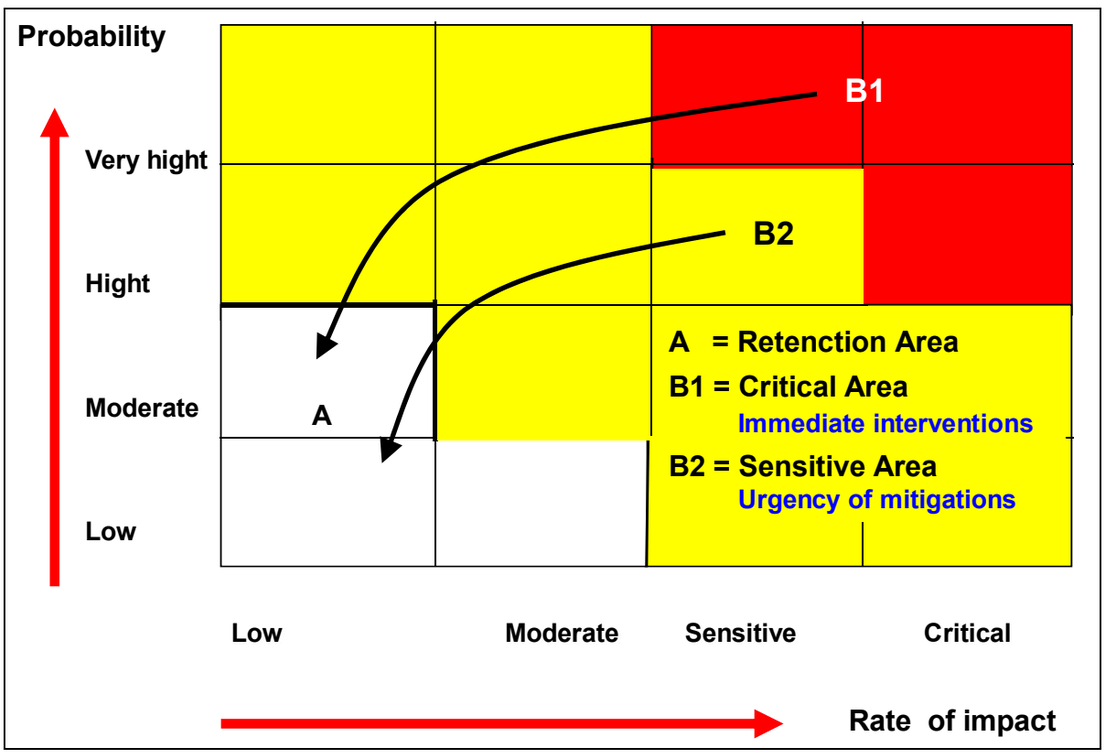


Fig. 4. Levels of risk acceptance.

Risk are always understood in relation to overall business opportunity and appetite for risk. Sometimes risk is compensated by opportunity (ENISA 2009 p.22). The European Network and Information Security Agency (ENISA) in its report regarding Cloud Computing Risk Assessment.

The risks identified in the assessment are classified into three categories:

a. Policy and organizational risks;
b. Technical risks;
c. Legal risks;

5. The ABBO's Information Models for Security – A.I.M.S.

A system is a collection of interacting components, policies and procedures that are integrated and organized to react to an input and produce a predictable output and have a feedback. Everything is not a part of the system is called the surroundings (Rogers B.B., 2006 pp. 67-71). The components themselves and the relationships among them determine how the system works.

A complex system is defined as a diverse system of sub- systems working together toward a common goal.

Complex systems may be deterministic or probabilistic. The goal of deterministic system is to produce the same output every time given a specific input. The performance of a deterministic system can be modelled and predicted by mathematical tools such as algebra and calculus. On the other hand, probabilistic systems do not always produce the same output, but rather a distributed output with a central tendency.

The ICT Security Company's System is the core model of A.I.M.S. family. It is made of three sub – systems like three entities in a close market how it is illustrated in Figure 5 (Abbo, Sun, Feb 2009 pp 195 – 200).

The first entity is "ICT security mission" a manufacturer of the other two entities considered customers: "Information mission" and "Company's mission" We should consider Company's mission an external running business engaged internally in an innovation e-policy which dedicates resources and requirements to information and ICT security missions. When we talk about resources we mean all the instrumental items: money budgets, software, manpower, hardware, facilities, training, know-how capabilities, operating procedures etc. that can be full- time or par-time dedicated. All those assets are component of the "chain of value" of the company to fulfill its mission and it's possible to measure them like an income account in a fiscal period. The three entities are obviously well-founded on information.

The quantity of information is normally encapsulated in **business information flows** (**B.I.F.s)** the we can defined as a summation of Acts, Facts, Requested Information and Delivered Information in a given timing:

$$\frac{\Sigma \{\text{Acts, Facts, RI, DI}\}}{\Delta T}$$

The facts consist on the potential productivity of the infrastructural architecture and the acts all the human and automatic actions connected with the architecture.

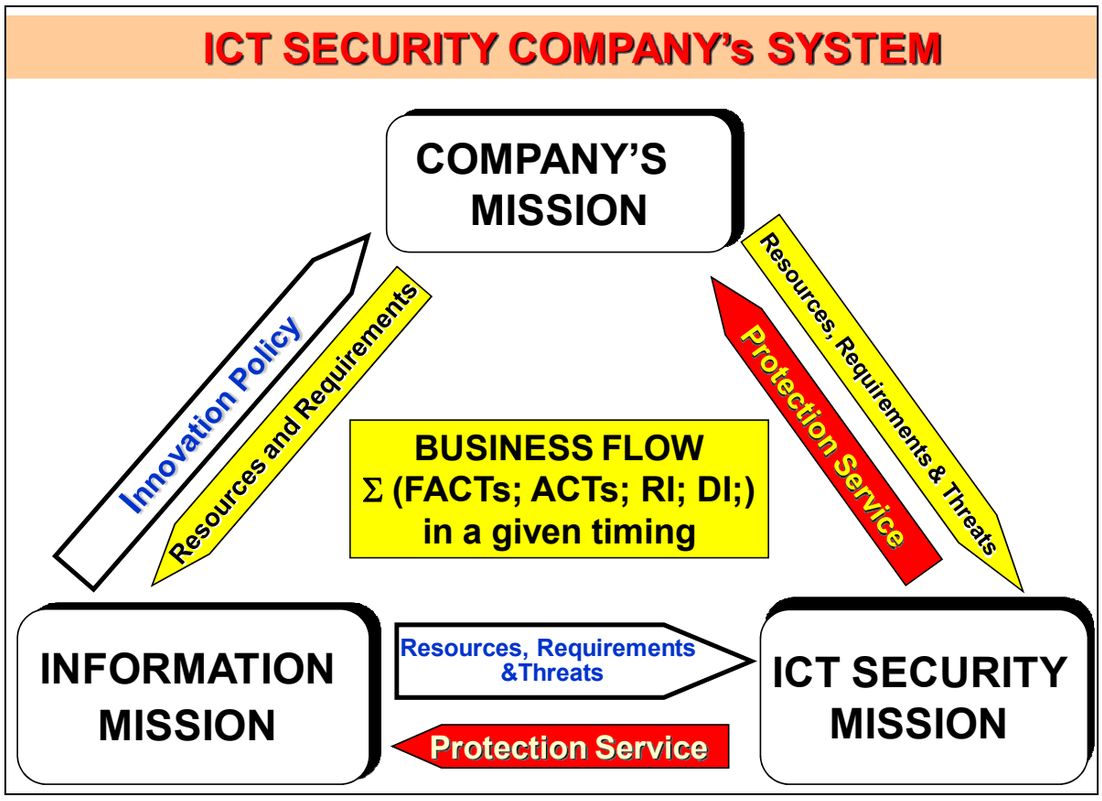


Fig. 5. The three missions are the entities of a close market where Company and Information are the two customers of Security Services.

"Information mission" is a pure deterministic system. It is designed to deliver business flows either on demand or automatically. Its competitive advantage is done by the effective business information flows per unit of time:

$$\frac{\text{Numbers of B.I.F.s}}{\text{Unit of time}}$$

"Company Mission" is both a probabilistic and deterministic system

It is designed to exploit the on – demand Business Information flows for a commercial objective either a service or a good. It is the only Mission in which there is the coexistence of pure risk (loss no-loss situation) and speculative risk (loss or gain situation). Its competitive advantage is done by the summation of profit per any Business Information Flow in the fiscal period:

$$\frac{\Sigma(\text{single BIF x its own profit})}{\text{Fiscal } \Delta T}$$

"**Security Mission**" is a pure probabilistic system. It's designed to protect the effectiveness of the business information flows according to the C.I.A. triangle. Its competitive advantage is done by One minus the probability of occurrence of a negative event divided by the functional cost of the Security Mission:

$$\frac{1 - P_O}{\text{Functional cost}}$$

The functional cost is defined like the percentage of resources of the business system budget that is invested for the defensive measures to protect the information (Author definition).

One of the key point is the that any instrumental item can have a multiple use one for each entity.

For instance an employer is dedicating his working time to Company Mission" but he/she is spending a percent of this working time to "Information mission" for duty purposes (e.g. production of digital documents, connection with the network) and smaller percent of time is dedicated at ICT Security Mission (e.g. unlock the door, enter the system with the password, updated the security software etc).

The focal point is that considering each single resource in terms of 100 percent functional units we can share it in three complementary slots. If we put on graphics the percent of each relevant resource that is dedicated respectively to the Information mission and to the ICT security mission we have the ISO-line of balanced budget (see Figure 6).

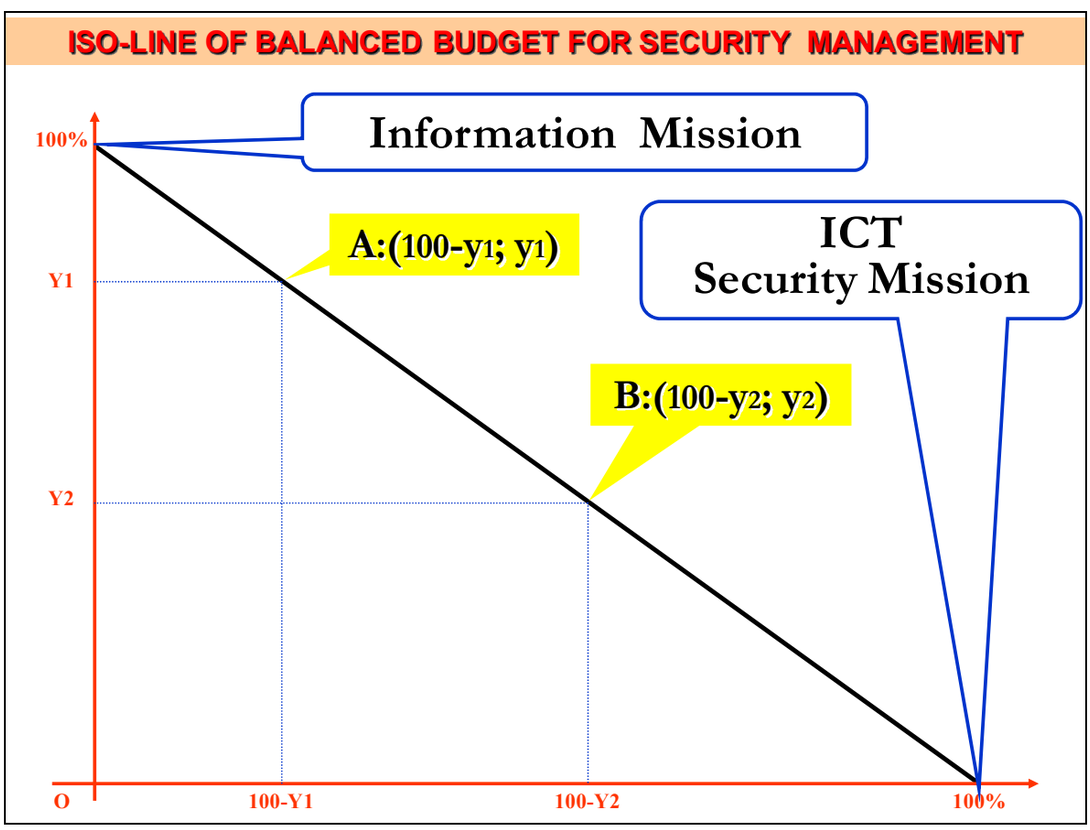


Fig. 6. The entire resources dedicated to IS systems are divided in two shares: the first rate is specific for information mission and the complementary one, dedicated to security, represents the functional cost. This graph representation belongs to the "two reciprocal exhaustive variables model". (Abbo, Sun, Nov 2009 pp 289 – 293).

Having several classes of resources, we should produce a graphic for each class of resource and compare in analytical context, or to use a mathematical system of nth equations. It should be outlined that the values in the graphic ranges from 0 to 100 and they are expressing percentage and the amount of resources that is given to ICT security mission is subtract from information mission budget. We should introduce the definitions of real cost and functional cost of the resources.

The real cost is the prize of a resource in the external market and is clearly represented in the balance sheet of the Company's mission. The functional cost is the percentage of each single resource that we should invest for the defensive measures of the resource for its operational survival.

By definition we can assume that ICT security mission represents the percentage of "Information mission" it should be employed for its survival and in an extensive sense to the "Company mission" survival. The real cost is measured in actual currency and ranges from zero to infinity, the functional cost it is a percentage ratio and ranges from zero to one hundred and by dimensions it is a pure number. Now we can associated, in the same graphic the ISO-line of balanced budget the curve of security performance: y = SP(x) that associates to every combination of functional cost of Information mission a point of security performance (see Figure 7). The combination of the functional costs is efficient only in the area represented by the integral of the realistic curve. The value of security performance is

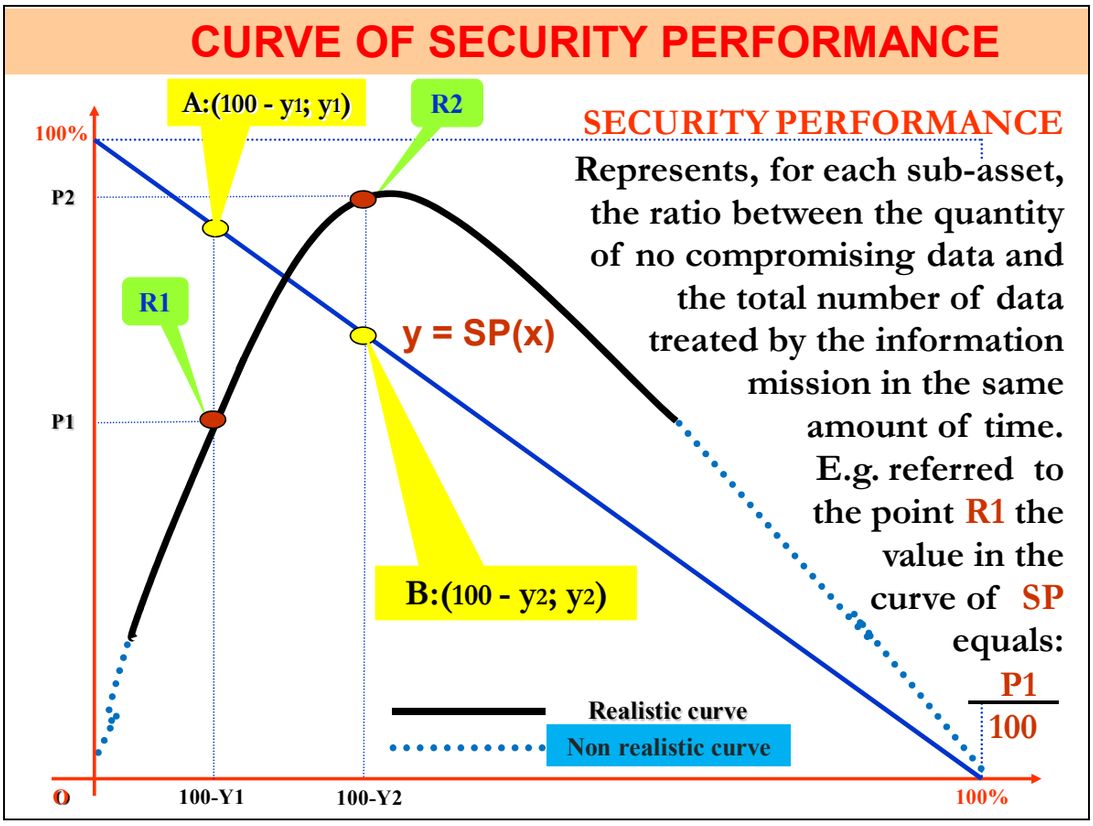


Fig. 7. The curve represents the level of security performance dependable from the functional cost. (Abbo, Sun, Nov 2009 pp 289 – 293).

represented by the ordinate of each point in the realistic curve that is a percentage value. The difference between one hundred and the value of security performance represents both the value of "threat performance" and the "quantitative risk analysis" for any model that has same premises and surrounding conditions.

The calculation of functional cost should be something of relatively easily to individuate in a strictly accounting way and its acceptance as an analytical tool addresses any possible scenario represented by all the families of security performances in every Information System (IS) context. In addition any change in the security architecture of an existing or projected Information System should take always into consideration both the functional cost and the rate of security performance..

By an analytical point of view that means to draw the curve **y = SP(x)**: the functional cost is fixed but the correspondence with the value of Security Performance Curve is variable that should be conquered on the field. While functional cost and security performance rates are variables that should be considered in the strategic planning, the dynamic confrontation is related to the operational planning. The tactical context should be tailored, in the middle period, for monitoring intrusions in order to:

- create a continuative operational feed back for a better security proficiency;
- match together the quantitative and qualitative risk analysis;
- create a kind of "field continuative intelligence" versus the Threat attempts and breakages.

The current use of data mining investigations and link analysis techniques it can be proficiently integrated with the "broader intelligence of the "Company's Mission" or with any allied IS security systems. Actually all the domain is largely unexplored in the sense that the "IS intelligence abilities" are mainly used in the relations either between the Information and Company missions or between the Company mission and its delivering customers. In the other hand the reporting capacity for IS security purposes ranges mainly in the operational planning for "daily purpose statistics".

The implementation of the same existing process between the Information and Company missions like CRM, Business intelligence and the appropriate definition of indicators and warning will be a proper way to close the security loop for any implementing stage of security governance. The capacity of reporting like any "measurable issue" is limited by two main considerations. The first is the capacity of measurement both by a technical and by a managerial point of views. In the specific case the reporting capacity of the security disruption (or attempt of intrusion) should consider if the technological tools can be proficient enough and if its employment on a large scale can create managerial bias on the of IS architecture governance. The second is the willing, the needs or the convenience of the Company mission management to implement a reporting process function in the tactical domain, the threshold of implementation and the level of accuracy.

6. The ASThMA (ABBO's Security Theoretical Measurement Algorithm)

Actually, in a given Information Security System, the implementation view should go deeper in the organizational aspects, creating operational patterns that are always dependable from "functional cost" and "security performance" (Abbo, Sun - May 2009 pp 342 -346).

A way to build-up operational patterns is to consider the Information domain that needs to be secured like horizontal interlocking sets, each one with its technical, organizational and formal security issues. The sets can be considered the domains of the pertinent situation Each domain has its functional cost and a class of security mitigation measures that can be considered mathematical variables. The mitigation measures belong to two main categories:

- Preventive measures that reduce the probability of a negative event on the Y- axis of the previous figure 4
- Protective measures that reduce the rate of impact in case of occurrence of a negative event on the X- axis of the previous figure 4

Any domain can be seen as a mathematical function that links the implementation of the measures with a probability of occurrence or a reduction percentage of the rate of impact .

In the Y-axis we should have n-integrated domains and for each one a function that states: the probability of effectiveness of the security system versus a negative event and/or a category of homogenous negative events is function of the interaction of the implemented preventive measures:

$$P_E = f(Pm1; Pm2; \ldots..Pmn)$$

The mathematical union of all the domains is given the global probability of the effectiveness of the security system. This mathematical union equals an algorithm called ASThMA and the results can be put on the pertinent matrix (table 2)

Pertinent parameters / Domains	**Functional cost**	**1 – P_E**	**P_A**	**P_O**
1st Domain	%	%		%
2nd Domain	%	%	%	%
(Nth-1) Domain	%	%	%	%
Nth Domain	%	%	%	%
Mathematical Union of all Domains	%	%	%	%

Table 2. The ASThMA matrix for preventive measures. All the numbers are percentage value. PE represents the probability of effectiveness of security system, PA the probability of an attack and PO the probability of a negative event and/or a category of homogenous negative events.

A similar assumption can be done also for the domain of X-axis where the generic probability is substituted by the percentage rate of impact of a negative event and/or a category of homogenous negative events is function of the interaction of the implemented protective measures(table 3).

It should be remarked that in each domain there are quantitative variable that can be expressed with a numerical entity and qualitative variables that can be expressed with an on/off implementation and a coefficient of quality. It is important to establish the appropriate indicators that reflect aspects of situation and which calculation is done by mathematical formulas. The set of indicators is called A.S.I.A. (ABBOs' Security Indicators Array). The validation of those indicators consists in their usefulness for a dual reason:

Pertinent Parameters / Domains	Functional cost	Percentage of pure damage reduction	Cost of resilience	Time of resilience	Consequential damages
1st Domain	%	%	**Currency**	**Δt**	%
2nd Domain	%	%	**Currency**	**Δt**	%
(Nth-1) Domain	%	%	**Currency**	**Δt**	%
Nth Domain	%	%	**Currency**	**Δt**	%
Mathematical Union of all Domains	%	%	**Currency**	**Δt**	%

Table 3. The ASThMA matrix for protective measures. It takes into consideration for every domain the functional cost, the percentage of immediate damage reduction, the cost and the time of reset (resilience parameters) and consequential damage of a negative event and/or a category of homogenous negative events. The consequential damages consider a future percentage reductions of Company Mission (loss of image, business activity etc.).

- the creation of a metrics, independent from the technology, that immediately give evidence links among security architectural safeguards, risks for the architecture and the business purpose of the architecture, surrounding environment and negotiation power with the treat;
- the frame (upper and lower level) for international security recognized standard-A.S.I.A. is including , but are not limited to, the following set of indicators

TPP - Threat Penetration Power indicator

$$(\Sigma Ei\ At)\ Ka\ /\ Tp \quad \text{where}$$

Ei Numbers of events that should take place for the threat reaching its aim
At Skilfulness coefficient that ranges from 0 to 1
Ka Time of alert for any event that should take place for the threat reaching its aim
Tp Penetration time of the threat

TM - Threat Motivation indicator =

$$Tib\ /\ \Sigma Ei\ Twc \quad \text{where}$$

Tib Incoming benefits that the threat has after reaching its aim
Ei Numbers of events that should take place for the threat reaching its aim
TwcWorking costs that the threat should afford for any single event;

TR - Threat Deterrence indicator =

$$Pt\ \Sigma Ei\ Twc \quad \text{where}$$

Pt Penetration time of Threat;
TwcWorking costs that the threat should afford for any single event

RE - Resilience Elasticity indicator

Rc /Ti where

Rc Cost of reset. After a negative vent
Ti Total income of the business supported by the information system

Fc **Functional cost** It is the percentage of resources of the business system budget that is invested for the defensive measures to protect the information. It is a number that ranges from 0 to 100

WoS - Weigh of System indicator

= Cs /Ti where

Cs Cost of safeguards
Ti Total income of the business supported by the information system

$\mathbf{P_o}$ Probability of occurrence

$\mathbf{Cp_o}$ Conditional probability of occurrence. It is the probability of a further negative event, given the occurrence of an initial negative event.

All the previous indicators should be abstractedly applied to any information architecture independently of the employed technology.

7. Conclusion

The aforementioned paragraphs set out some fundamental aspect linked to security and risk analysis.

Firstly security is framed as a engineered system where the input is a malevolent human attack upon a business architecture and the desired output is a defeated adversary and an intact asset. In the design of the engineering security system the desired output is the risk evaluation and expressed by numbers that are the result of the formula likelihood or probability of occurrence and severity of the consequence(s) both normally express qualitatively.

Secondly the three pillars (C.I.A. triangle) are seen as a whole **and not specifically considered as a multiple value entity** and consequently the investments and the implementation of safeguards are indiscriminate. It would be more appropriate to link the value of availability, confidentiality, and integrity with the asset and liability statement for any class or set of information, at the end of the suitable working timeframe.

Thirdly the security system **is not considered as an economical system** in the sense that there is no leverage between performances and investments. The implementation of safeguards in an information system match the risk reductions in the supported business system but it is not compared with the Return of Investment (ROI) of the information safeguards. That is a consequence of the shortcoming of the above mentioned system feedback.

Fourthly The implementation of safeguards in an engineered system increase the weight of the system itself and bias the efficiency of the mission.

Fifthly the increasing inter-connections between IS systems **makes more and more difficult the estimation (and by consequent he management) of a given risk** by the traditional statistical and /or among different information infrastructures.

The purpose of seeing the IS security models (like the ICT Security Company's System, the formula of Security and all the others mentioned in the publication) is to create a scientific approach to understand the nature of Is security issues, and to manage the connected problems in the most possible consistent way. The main advantage of an analytical approach is not only the possibility of always estimating costs, but also proficiency, adaptations and re-usability of an IS security architecture. Actually the IS security is perceived as a common sense knowing where the dominant perception is linked to experience; but the build-up of security performing rules requires a point of view beyond the pure empirical reports. The main perspective of IS security analysis is to create a "reference lay-out, in order to make global, measurable and repeatable lay-outs.

The creation of models should be done by accurately considering and analyzing also the growing of interdependency of the complex integrated information systems that will continue and accelerate as more technologies are integrated to deliver rich services. Today we have no way to globally model, understand, monitor and manage the risks presented by the growth of these systems in other words to have the risk assessment in the forensics domain.

The build-up of an interactive set of controlled models is the most suitable way for maintaining a "risk estimation forensics capacity" that should be able to evaluate, make real-time understandable, monitor and manage the measured rate of the security defensive profile of interconnected systems, align information architectures with organizational goals, and help these process to cooperate.

The applications are inclusive of all the IS architecture and a scientific analytical approach should became a the necessary doctrinal baseline when entering in an unplanned "systems of systems" where functionality override resilience.

The impact of implementing the above mentioned solutions in terms of social, political, economical costs compared with the improvements of market benefits and if it is taken seriously by the Government can positively influence the GDPs

8. References

Abbo D. – Sun L. (Feb - 2009) "*Security analysis of information systems*" IADIS International Conference - e-Society Proceedings Vol II – Edited by Piet Kommers and Pedro Isaìas Barcellona – SPAIN.

Abbo D. – Sun L. (May - 2009) "*The patterns for information system security*" ICEIS 11th International Conference on Enterprise Information Systems- Proceedings of Information System Analysis and Specification – Edited by Josè Cordeiro and Joaquim Filipe Milan – ITALY.

Abbo D. – Sun L. (Nov - 2009) "*The information infrastructure protection anlysis*" IADIS International conference - Proceedings of Applied Computing 2009 vol.II– Edited by Hans Weghorn, Jörg Roth and Pedro Isaìas Rome – ITALY

Barker C. W.(2006) *E-Government Security Issues and Measures* - HANDBOOK OF INFORMATION SECURITY vol. 1, Editor- in-Chief Hossein Bidgoli published by John Wiley & Sons NJ USA

Broder, J.F. (1993) *Encyclopaedia of Security Management* – Techniques and Technology, Butterworth-Heinemann, Burlington MA USA.

Brotby W. C (2009) *Information Security Management Metrics – A definitive guide to effective security monitoring and measurement* Auerbach Publications Boca Raton FL US

CSA – Cloud Security Alliance – (2009), *Security guidance for critical areas of focus in cloud computing V2.1* – URL http://cloudsecurityalliance.org/csaguide.pdf

CSA Guidance – Cloud Security Alliance – (2009), *Security Guidance for Critical Areas of Focus in Cloud Computing*- URL http://cloudsecurityalliance.org/guidance.html

Douglas M. (2005) *Risk and blame* - Routledge NY, USA.

ENISA -European Network and Information Security Agency- (2009) *Cloud Computing Risk Assessment* -- URL: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

Hyperdictionary *Meaning of National Information Infrastructure* -- URL: http://www.hyperdictionary.com/computing/national+information+infrastrucure.

Innamorati, F. (2002) *La security d'impresa*, Insigna Edizioni Simone, Milan ITALY

ISO/IEC, Guide 73 (2002) *Risk management - vocabulary – guidelines for use in standards*, Geneva CH.

ISO/IEC, 27001 (2008) "*Information technology – Security techniques – Information security management system – Requirements*" Geneva CH

ISO/IEC, 27005 (2008) "*Information technology – Security techniques – Information security risk management – Annex E: information security risks assessment approaches*" Geneva CH.

Jones A. – Ashenden D. (2005) *Risk management for computer security*, Elsevier Butterworth-Heineman, Oxford UK

Lam J. (2003) *Enterprise risk management – from incentives to controls*, John Wiley and Sons, NJ USA

Manunta, G. (2000) *Defining Security* Diogenes paper n.1 Cranfield Security Centre– The Royal Military College of Science, Hampshire UK

Rogers B.B. (2006) *Engineering Principles for Security Managers* – THE HANBOOK OF SECURITY Edited by Martin Gill – Palgrave Macmillan, London, UK .

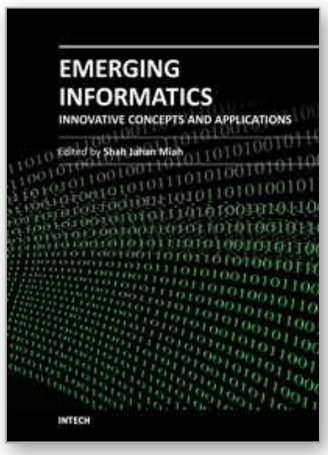
Rogers, R. (2005) *Network Security Evaluation using the NSA-IEM*, Syngress Publishing Inc. Rockland, MA - USA,

Slade R. (2006) "*Dictionary of information security*" Syngress Publishing Inc. Rockland, MA - USA

Tipton F. H. – Henry K. (2007) *Official (ISC)2 Guide to the CISSP CBK*, Auerbach Publications New York - USA

Tsohou A., Karyda M., Kokolakis S., Kiountouzis E. (2006) "*Formulating information systems risk management strategies through cultural theory Information*" - Management & Computer Security Vol. 14 N° 3

Whitman, E.M., Mattord, J.H., 2008. *Management of Information Security*, Thomson Course Technology, CANADA, 2nd edition.



Emerging Informatics - Innovative Concepts and Applications

Edited by Prof. Shah Jahan Miah

ISBN 978-953-51-0514-5
Hard cover, 274 pages
Publisher InTech
Published online 20, April, 2012
Published in print edition April, 2012

The book on emerging informatics brings together the new concepts and applications that will help define and outline problem solving methods and features in designing business and human systems. It covers international aspects of information systems design in which many relevant technologies are introduced for the welfare of human and business systems. This initiative can be viewed as an emergent area of informatics that helps better conceptualise and design new world-class solutions. The book provides four flexible sections that accommodate total of fourteen chapters. The section specifies learning contexts in emerging fields. Each chapter presents a clear basis through the problem conception and its applicable technological solutions. I hope this will help further exploration of knowledge in the informatics discipline.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen