7

A Comprehensive Risk Management Framework for Approaching the Return on Security Investment (ROSI)

Elvis Pontes, Adilson E. Guelfi, Anderson A. A. Silva and Sérgio T. Kofuji
Laboratory of Integrated Systems, Polytechnic School at the University of São Paulo, Brazil

1. Introduction

For designing cost-effective security strategies, organizations need practical and complete frameworks for security and risk management (RM), with methods for measuring and managing risks within organizations. In the recent years computer systems have become more present in all economic fields, improving activities in the industry, commerce, government, and researching areas. For the near future the same growing rate of cyber technology is projected for all those areas (Federal Information Security Management Act [FISMA], 2002). On the other hand, threats for this new way of doing business are also growing significantly: hackers, computer viruses, cyber-terrorists are making headlines daily (Internet Crime Complaint Center [IC3], 2008). Consequently, security has also become priority in all aspects of life, including business supported by computer systems (Sonnenreich et al, 2006).

In this reasoning line, some major points may worry researchers, technology implementers, decision makers and investors: 1) the framework to be adopted in organizations for making business secure; 2) managing security and risk levels in organizations for making business workable; 3) mainly, the return of security investment has to be measured to make business profitable.

For business, when the topic is security, it is hard not to consider the associated financial aspect, as any other costs (time, processing, electric power, throughput, etc.) (Pontes et al, 2009a, 2009b, 2009c, 2010). However, for the decision makers it does not matter whether firewalls or soldiers are going to protect the Enterprise Resource Planning (ERP) system and/or other servers. Instead, decision makers have to be aware of the costs related to security and the consequences on the bottom line, both for the present day and for the time yet to come (Sonnenreich et al, 2006). So, it is important that Information Technologic (IT) and Information Security (IS) professionals to be aware about how to justify costs and investments in IS (National Institute of Standards and Technology [NIST] SP800-65, 2005), (International Standardization Organization, [ISO] TR 13569, 2005). Besides, all the related security costs must be correctly presented faced to the real necessities. Risk Management (RM) and Risk Analysis (RA) are efficient means for both: to show the needs of protection and the impact in the overall business activity (ISO 13335, 2004), (ISO 27005, 2008). Usually employed together with RM, the Cost-Benefit Analysis (CBA) may identify the cost-effectiveness for the security countermeasures, supporting the statements of the IT or IS

professionals (e.g. technology implementers) during the approval process of implementations of IS controls, as Intrusion Detection Systems (IDS), biometric controls for access control, etc. In a software based environment, the CBA may similarly be used to apply one or more controls (Wei et al, 2002). The reason of CBA is to present the benefits of IS controls (countermeasures) that may be adopted, comparing to the costs of each IS mechanism.

When CBA is applied, it is intended to determine the intrinsic cost of the IS control, correlating it to the overall organizational environment and analyzing the systemic consequences of IS controls adoption. For instance, by the use of CBA it is possible to track hypothetical overhead because of IS controls employment, before the use of the controls. It is also important to emphasize that during the CBA of a IS control it is possible to assess the positives about the control, e.g.: the increment of selling due to the use of Public Key Infrastructure (PKI) in the electronic commerce.

Another important approach to assess IS mechanisms and IS controls is the Return on Security Investment (ROSI), which analyzes different points if compared to CBA. ROSI concerns the idea about historical series of incidents that were problem to productivity rates to the organizations (Sonnenreich et al, 2006). ROSI concerns also the cost avoidance resulting from resistance, recognition, and reconstitution efforts for the IT infrastructure in the organization (O'Neil, 2007), based on the Annualized Loss Expectancy (ALE) and the number of incidents (Wei et al, 2001), (Government Chief Information Office [GCIO], 2004), (O'Neil, 2007). In spite the fact that ROSI may be used to justify costs and investments in organizations (GCIO, 2004), ROSI is partially accepted in IS. (Heiser, 2002) mention that there is no way for calculating an effective ROSI, but superficial estimations may be done. While regular ROSI methods consider the likelihood of security incidents (ALE), they do not approach studies about forecasts and trends of incidents or unwanted events, like unwanted Internet traffic (Pontes et al, 2009a, 2009b, 2009c, 2010).

The goal of this chapter is to propose a comprehensive RM framework, in which the traditional approach (with the establishment of risk levels to attend the business requirements) is extended to add a new phase for handling variables concerning ROSI statements. As a result we intend to address the impact of the comprehensive RM framework over the traditional RM in IS, in order to obtain cost-effectiveness of IS controls, reducing uncertainties and risks in IT environment, and finally improving the probability of positive rates of ROSI.

The comprehensive RM framework includes the CBA (Wei et al, 2001) and ROSI (GCIO, 2004), (O'Neil, 2007), which analyzes the incidents history, ALE, and productivity rates. This chapter is organized as follows: RM is presented in section 2. Section 3 regards ROSI models. The description of the comprehensive RM framework is in the section 4. Section 5 and 6 summarizes analysis and conclusions respectively.

2. Risk management (RM) – traditional frameworks

Traditional frameworks for RM regard models that do not consider phases to handle ROSI issues in IS environments. Generally, traditional RM frameworks deals with the needs of protection and the impact in the overall business activity.

Government and society are more and more concerned about eventual loss of data, theft of information and with possible loss of human life due to failures in computer systems. Consequently, IS and IT have been focused by diverse standardization organizations, as

International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), British Standards (BSi), Australian/New Zealand Standard (AS/NZS), Project Management Institute (PMI), Brazilian Society for Technical Standards (ABNT), Information Security Forum (IFS), among others. The main recommendations about IS reinforce the adoption of good practices for RM in IT systems. The most well known recommendations for IS are the BS 7799 series (British Standards Institute [BSi], 1999), (BSi, 2002) and (FISMA, 2004). The BS 7799 series were developed by the British Government and are cited as good practices for managing IS systems. Lately, the first documents from the BS 7799 were revised and reorganized in the ISO17799 series (ISO 27005, 2008).
The public American law 107-347 (e-Government Act) 2002, recognizes the importance of IS to the interests of the economy and national security of United States (FISMA, 2002). The third title of the law, called FISMA, imposes that each federal agency has to develop, document and implement an extensive program for management IS. (FISMA, 2002) is supported by diverse NIST documents.
Currently, new efforts for revising IS standards are happening, and they are going to be reclassified in the ISO/IEC 27000 series. The objective is to align the IS management standards with the ISO 9000 and ISO 14000 series. The structure of ISO 27001 is likely FISMA, as they are cyclic models intending the ongoing Risk Management for identifying, evaluating, controlling, monitoring, reducing and/or accepting risks. Fig. 1 presents an overview of some RM and IS management standards, as the relation among each other.

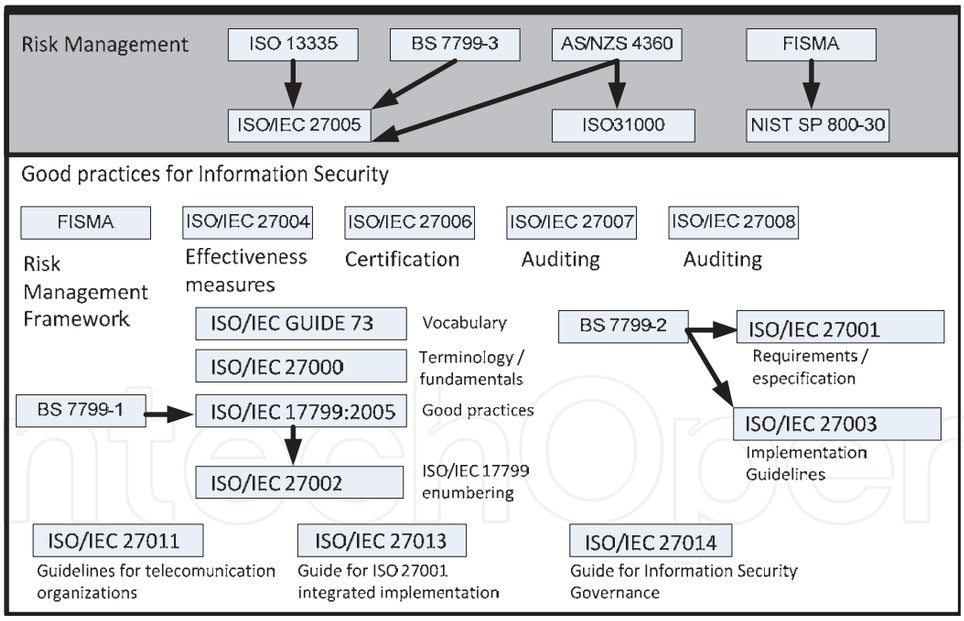

Fig. 1. Evolution of RM and IS Management

According to Fig. 1, some of the RM standards are the ISO 13335, BS 7799-3 AS/NZS 4360, FISMA, ISO/IEC 27005, ISO 31000 and NIST SP 800-30.
(BSi 7799-2, 2002) defines the fundamental concepts and the vocabulary for IS to be used in the documents of the ISO 27000 series. The adopted terminology in most of the IS standards derives from (ISO 73, 2009). (ISO 27001, 2006) and (ISO 27002, 2005) are based on BS 7799-2 and ISO 17799-1. The recommendation ISO 27001 introduces a model to establish,

implement, operate and supervise, to analyze critically, to maintain and to improve a IS management system. ISO 27002 (formed ISO 17799:2005) introduces IS concepts and discusses about motivations for establishing IS management within organizations. In most parts of the document, the IS best practices are detailed and associated to the objectives of the IS controls mentioned in the ISO 27001. The preliminary version of ISO 27003 is derived from the BS 7799-2 annex B, and is basically a guide to implement the management IS system.
RM is founded on principles and good practices for management and security, to support the decision making processes (NIST SP800-30). More details about the RM standards can be found in the following subsections.

2.1 AS/NZS 4360, ISO 31000, ISO 13335 and ISO 27005

(Australian and New Zealand [AS/NZS], 2004) and (ISO 31000, 2009) define risk as everything that deviates from de main objective. This concept is directly associated to the strategic goals of organizations. ISO 31000 offers an integrated RM model to the organizations, providing a holistic view about risks to the RM members (stakeholders) to improve the decision making process. Fig. 2 illustrates the constant integration among each stage of (AS/NZS, 2004) and (ISO 31000, 2009), and each stage can be described as follows:

- Communication and consultation: this planning stage concerns any stakeholder involved with the RM, in both cases: internal and external to the organization. During the planning stage, all problems related to risks, consequences of impacts and the management actions must be presented;

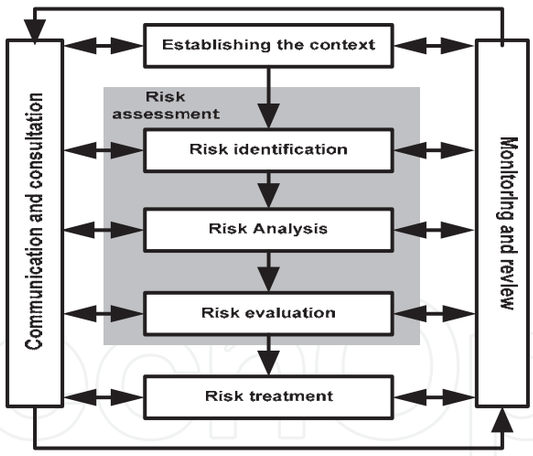

Fig. 2. RM – ISO 31000 and AS/NZS 4360

- Establishing context: stage to align the RM with the organizational culture, internal and external processes and other criteria (as risks criteria, roles and responsibilities, likelihood metrics, levels of acceptance, etc.).
- Risk Assessment: integrated process for identification of risks, RA and risks evaluation. It includes: 1) Risks identification: based on the objectives and criteria defined during the context establishment, relevant risks to the organization are identified throughout this stage; 2) RA: phase for determining causes and sources of risk, as well as occurrence likelihood and impact; 3) Risk Evaluation: based on the results of the

previous AR, this phase proposes a comparison between the estimated risks and the risk criteria to determine the risk level.

- Risk Treatment: process regarding selection and implementation of safeguards to modify risks;
- Monitoring and review: refers the changing analysis and / or trend tracking, periodic auditing, incident registering and maintaining security logs.

AS/NZS 4360 and ISO 31000 are cyclic models, with constant feedback done during the monitoring and reviewing, as well during the communication and consultation stages. In other hand, as Fig. 3 depicts, the RM model proposed by the (ISO 27005, 10) is very similar to the model presented by Fig. 2, having few nuances which can be noted, e.g., the decision points and the risk acceptance phase which trigger the beginning of the model and/or the monitoring/communication phases. Even though, ISO 27005 has one stage for risk treatment, neither ROSI, nor hypothetical closing situations (sunset in accordance with (NIST SP800-21, 2005)) are deeply commented or recommended in these standards.

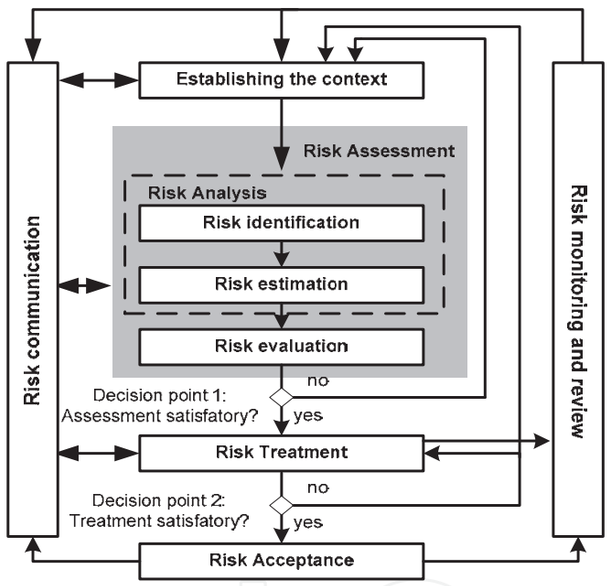

Fig. 3. RM – ISO 27005

2.2 FISMA and NIST SP800-30

The risk-based approach to security control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, executive orders, policies, standards, or regulations (FISMA, 2002). The following activities related to managing organizational risk (also known as the NIST RM Framework) are paramount to an effective IS program and can be applied to information systems within the context of the enterprise architecture (see Fig. 4):

Step 1: CATEGORIZE the information system and the information resident within that system based on impact. FIPS 199 and NIST SP 800-60;

Step 2: SELECT an initial set of security controls for the information system based on the security categorization (FIPS 199) and the minimum security requirements (FIPS 200); apply tailoring guidance as appropriate; and supplement the tailored baseline security controls

based on an assessment of risk and local conditions including organization-specific security requirements, specific threat information, cost-benefit analyses (NIST SP800-30 and NIST SP 800-53).

Fig. 4. RM – FISMA

Step 3: IMPLEMENT the IS controls.
Step 4: ASSESS the security controls using appropriate methods and procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. NIST SP 800-53A
Step 5: AUTHORIZE information system operation based upon a determination of the risk to organizational operations, organizational assets, or to individuals resulting from the operation of the information system and the decision that this risk is acceptable. (NIST SP800-37, 2010)
Step 6: MONITOR and assess selected security controls in the information system on a continuous basis including documenting changes to the system, conducting security impact analyses of the associated changes, and reporting the security status of the system to appropriate organizational officials on a regular basis. NIST SP 800-37 and SP 800-53A.
Among the standards and for the NIST's RM Framework, NIST SP800-30 (RM Guide for IT) provides guidelines for RM with definitions and necessary directions to assess and lessen identified risks in IT systems (NIST SP800-30, 2002). NIST SP800-30 comprises in two phases: risk assessment (system characterization, threat identification, vulnerability identification, control analysis, likelihood determination, impact analysis, risk determination, control recommendations, results documentation) and risk mitigation (prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process). But, neither ROSI, nor hypothetical closing situations is referred in any (FISMA, 2002) and (NIST SP800-30,2002).

2.3 Project management body of knowledge PMBOK

PMBOK approaches RM in a project matter, including processes related to conducting RM plans, identifying risks, risks analysis, response, monitoring and control (PMBOK, 2008).

Most of processes are updated during the project life cycle. The RM objectives are: to increase the probability and impact of positive events, to reduce de probability and impact of negative events to the project. According to Fig. 5, RM concerns the following steps:
1) RM planning (decisions about how to approach and to execute the activities during the RM in a project; 2) Identifying risks (to determine which risks may affect the project, documenting the risks' characteristics); 3) Qualitative RA (prioritizing risks for further analysis or action by assessing and combining their probability of occurrence and impact); 4) Quantitative Analysis (process of numerically analyzing the effect of identified risks on overall project objectives); 5) Plan Risk Responses (process of developing options and actions to enhance opportunities and to reduce threats to project objectives). 6) Monitor and Control Risk Responses (the process of executing risk response plans, tracking identified risks, monitoring residual risks, identifying new risks, and evaluating risk process effectiveness throughout the project).

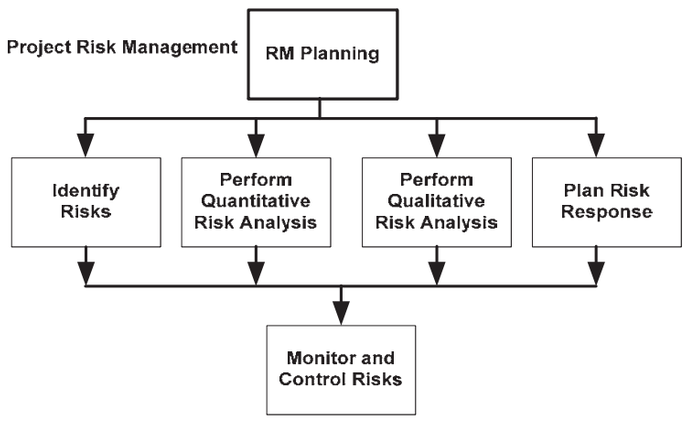

Fig. 5. RM – PMBOK

Even though (PMBOK, 2008) considers forecasting for other areas of projects (as evolution performance, estimative about finalization - time and cost), neither ROSI, nor forecasting of incidents trends, nor hypothetical closing situations for RM are referred in (PMBOK, 2008).

3. Return on security investment (ROSI)

ROSI concerns the idea about historical series of incidents that were problem to productivity rates for the organizations, the cost avoidance resulting from resistance, recognition, and reconstitution efforts for the IT infrastructure in the organization (Wei et al, 2001), based on the ALE (Pontes et al, 2009a), (GCIO, 2004), (O'Neil, 2007). ROSI with forecasting combines the conventional ROSI with hybrid prediction techniques (Pontes et al, 2009a, 2009b, 2009c, 2010). Some models for conventional ROSI and ROSI with forecasting are shown in this section.

3.1 ROSI - cost-benefit model

This model was developed to handle intrusions and unwanted traffic with an IDS, considering the cost-effectiveness of the countermeasure.
Most of the current ROSI methods refer to the work of (Wei et al, 2001), about cost-benefit analysis in IDS, considering it as one of the bases for the ROSI methods (Sonnenreich et al, 2006), (GCIO, 2004), (O'Neil, 2007).

(Wei et al, 2001) says that a cost -effective analysis about the IS controls with a study of the costs is the first step toward to the cost-benefit analysis in the IT environment. Then, the major intention of (Wei et al, 2001) was to build a methodology with a cost-benefit model, based on investigation of cost factors and categorization of some variables of the environment. The proposal could be used either for quantitative estimative, or qualitative costs, to determine the best choice for the cost-effectiveness (cost-benefit).

This methodology needs a previous RA to define the scope and the needs of IS controls to the organization assets, taking into account the values and vulnerabilities of each asset and the relevant threats. Lastly, the methodology includes likelihood about the incidents occurrence – when risk becomes impacts to the organization. This prognostic must be managed and controlled. Then, the ALE is calculated. The cost-benefit analysis is the next step: it works like a tool for the IDS, helping to determine whether, or not, the IDS adopts countermeasures to stop the intrusion. According to (Wei et al, 2001), it is not suggested to employ an extremely restrictive posture, as the cost of such posture is going to be more expensive then the benefit it could bring. The cost factors are determined from the RA and are divided as damage cost, operation costs and response costs. Then these costs are combined to determine the total cost for each intrusion.

The damage cost represents the maximum amount of damages that an attack may cause to an asset, when the IDS and other controls are not effective. The response cost relates to actions taken against the intrusions, including actions to stop the intrusion and to reduce damages. These actions, or controls, must be defined in the RA, according to the mapped threats. Operation cost is the processing of the event flow being monitored and analyzed in the IDS. After the cost factors definition, the cost values can be acquired when the RA is executed, leading the complementation of the cost matrix. Finally, the cost model may be applied as in (1):

$$Cost\_total(e) = \sum_{i=1}^{N} (CostC + CostOper(e)) \tag{1}$$

The Cost_total(e) is the total cost, N is the number of the event and CostC is the consequent cost of the prognostic for a intrusion event and for the IDS, that is determined for the damage cost and response cost. There are five types of prognostics: 1) FN (false negative); 2) TP (true positive); 3) FP (false positive); 4) TN (true negative) 5) Misclassified hit.

So, it was created a model to analyze multiple hosts as (2):

$$Cost\_total(e) = \sum_{i=1}^{N} (\sum_{j=1}^{H} Cost\_Dam(i) + Cost\_\mathrm{Re}s(e) + Cost\_Oper(e)) \tag{2}$$

H is the number of attacked hosts. The cost model may be implemented in the IDS context as shown in Fig. 6.

According to Fig. 6, the Message Server collects data from other tools, managing the messages, verifying the intrusion and the log messages. If an intrusion incurs, the Message Server reports the intrusion, status, attacked asset and other important information to the Cost Model. The Cost Model analyzes the information and calculates the cost, comparing to other alternatives. Then, a message is sent back to the Message Server. If the cost to respond the intrusion is larger than the benefit, the Message Server labels the received information, but does not send it to the Alert Server. Otherwise, the information is sent to the Alert

Server and the Response Server. The message is shown in display. The Response server acts according to the Cost Model advice.

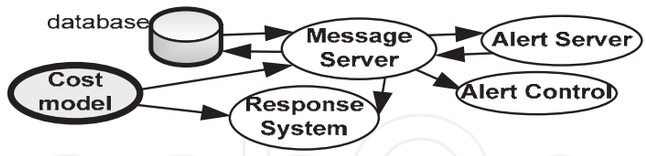

Fig. 6. Cost Model

This model has not yet undergone extensive enough training to be used in commercial applications. In addition to cost modeling and intrusion detection functions, the automatic response function is very important to the network intrusion detection system. With the cost model and automatic response system, a network IDS can both detect an attack and decide if it is worth stopping. If it is worth stopping the attack, the network IDS can automatically employ countermeasures. Even though (Wei et al, 2001) recommends a previous RA before applying the cost-benefit model, RM frameworks are not approached.

3.2 ROSI – GCIO Australia

This framework uses diverse approaches to obtain cost-benefit in SI countermeasures. Then, it is proposed a hybrid tool, combining ALE (Wei et al, 2001) with the Australian standard Threat and Risk Assessment framework (GCIO, 2004). The hybrid tool has also an extension to "Monte Carlo" statistical analysis (in electronic spreadsheet) of the possible spread in cost-benefit results arising – as security incidents vary randomly in their rate of occurrence and their severity (GCIO, 2004). "Monte Carlo" involves introducing variability into one or more parameters of a complex model, re-running the calculations many times and studying the ranges of resulting outputs

The framework also transforms qualitative judgments of likelihood and severity into quantitative appraisals of loss expectancy (ALE), with and without security. Fig. 7 presents the sequence of steps for running the (GCIO, 2004) framework. Each step has, in matter of fact, an electronic spreadsheet to be fulfilled, with some simple qualitative definitions and some estimative equations to transform qualitative into quantitative criteria.

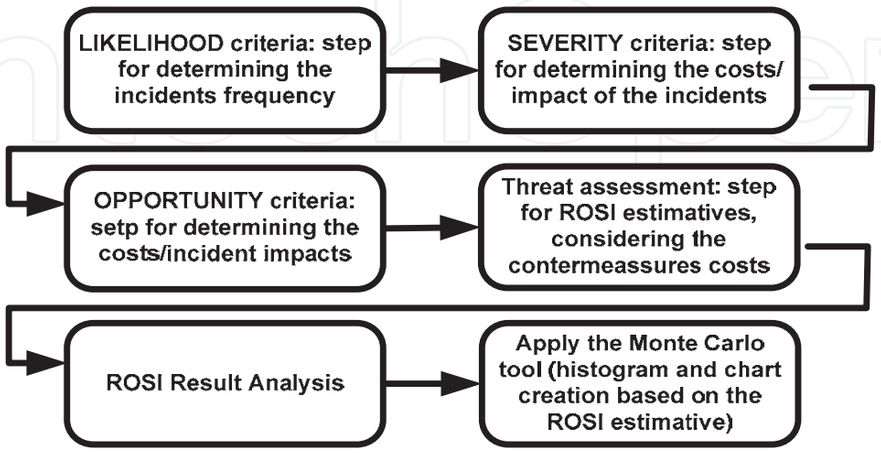

Fig. 7. GCIO ROSI framework

Even though the framework is easy to implement, it has some limitations, as follows: 1) Difficult to separate effects of countermeasures; 2) Restricted sources of randomness; 3) Difficult to predict how countermeasures affect severity; 4) Security incidents are not necessarily independent; 5) Hard to implement in a real time system.
Although steps of RA are performed in (GCIO, 2004), RM frameworks are not considered.

3.3 ROSI – Carnegie mellon and US department of homeland and security

The objectives of this method are to make a more real estimate about the ROSI, considering the absence of actual data on the number of incidents and to better assess the impact of an individual incident. According to (O'Neil, 2007), ROSI savings is divided by costs as (3):

$$ROSI = \frac{Savings}{Cost} \tag{3}$$

Savings is cost avoidance resulting from resistance, recognition, and reconstitution efforts. Cost includes preparation and incident cost. Incident cost is cleanup, lost opportunity, and critical infrastructure impact.
This model estimates if the expected number of incidents is low, the security readiness investment will be recouped; for a higher number of cyber attack incidents, what are the minimum factors needed to fully recoup security investment; if there is an equitable scheme for sharing security readiness costs among the project, the enterprise, and the government; and what are the guidelines for public-private collaboration and cost sharing. The method is divided in three different phases, with different steps for each one:

1. ROI 1
   a. Savings = (Resistance Savings + Recognition Savings + Reconstitution Savings)
   b. Cost = (Total Preparation + Total Cleanup + Total Lost Opportunity + Total Critical Infrastructure Impact)
2. ROI 2
   a Savings = (Full Cost Incurred − Cost with Avoidance)
   b Cost = (Preparation + Cost with Avoidance)
3. ROI 3
   a Savings = (Full Cost Incurred)
   b Cost = (Preparation + Cost with Avoidance)

Each one of the variables in the cost and savings, for ROI 1, ROI 2 and ROI 3, has a long definition and estimative to reach the correspondent value. The aim of this chapter is not to describe such procedure. Because of the long analysis for each variable, this method may not be effective in real time systems. This method does not consider RM frameworks.

3.4 ROSI – British computer society and Australian computer society

For this approach, the ROSI estimative has a direct relation to the productivity rates (Sonnenreich et al, 2006). Determining expected returns for security investments involves estimating the risk exposure and the amount a solution will mitigate the risk. As the security incidents are not successfully tracked in most organizations, the incidents history is an item not as important in this approach as it is in others.
A meaningful ROSI can be calculated by focusing on the impact security has on productivity. The productivity lost due to security incidents can have a serious impact on the bottom line. For many organizations the cost of lost productivity associated with a

security incident is far greater than the cost of data recovery or system repair, as it is shown in (4):

$$ROSI = \frac{Expected\_Returns - Cost\_investment}{Cost\_investment} \quad (4)$$

The cost of a solution must include the impact of the solution on productivity, since this number is often large enough to make or break the viability of a given solution.
The problem with this approach is that isolating security's impact on productivity from other factors (such as poor performance) is impossible. If the survey is correctly constructed, there will be a strong correlation between the survey score and financial performance. Specifically if a department shows a decrease in perceived downtime, it should also show an increase in productivity on the internal balance sheets. However, with a good survey and scoring system for productivity, combined with external measurements of intellectual property value, it becomes possible to quantify risk exposure in a repeatable and consistent manner.
Risk exposure is measured as the productivity loss due to existing security issues. This approach assumes that serious disasters are rare and hard to quantify but everyday incidents create a significant amount of aggregate loss. Solving these problems provides real returns and improves security at the same time, which has the side-effect of preventing some of those major disasters. This approach does not consider or RM frameworks.

3.5 ROSI – North Carolina A&T State university

Accordingly with (Al-Humaigani et al, 2003), it is necessary to evaluate security planning and security solutions, analyzing business needs and security controls to be employed. In this sense, ROSI must present the lowest possible values to address costs of security breaches and costs of security controls. Security controls can be classified in two types of costs: 1) relative cost for acquisition, implementation and maintenance; 2) costs from the limitations of users, environments and tools.
The objective of (Al-Humaigani et al, 2003) is to examine security costs, in order to detail ROSI analysis and thereafter to propose a model for quantifying the referred ROSI analysis. According to (Al-Humaigani et al, 2003), (Heiser, 2002), there is no a safe way to quantify ROSI, and the best argument is that the investment in security can prevent losses.
The usual justification for conducting risk assessments is to protect integrity, confidentiality and availability of information. Moreover, due to difficulties in quantifying security investment, often the justification is rooted in Fear, Uncertainty and Doubt (FUD). However, ROSI can be a tool for decision making process: 1) the ROSI analysis numbers can be used to justify the investment in security; 2) the ROSI can be used to indicate the type of investment required, such as technology or people; 3) the ROSI analysis numbers also can be used to set ranges and insurance values (eg. based on what is invested in security organizations).
Although, ROSI takes place before the implementation of security controls and lies on empirical data. The model proposed by (Al-Humaigani et al, 2003) includes several factors that may be related in obtaining ROSI, considering both the pre as post implementation and demonstrating which elements affect the assessments in ROSI. Qualitative justifications for investments in security should incorporate quantitative measures, producing robust ROSI numbers. The model should answer the following questions:

1. How much is for an organization to invest in information security?

2. How much is for an organization not to invest in information security spending.

The solutions presented by (Al-Humaigani et al, 2003) assess each one of the following varriables:

- CTI: The cost of procuring the security tool or software, its licenses, and upgrades.
- CT2: The cost of the extra physical hardware, rooms, and facilities needed.
- CT3: The cost of the training and the time of the human resources forcing the security policies and implementing the security tool.
- CT4: The losses due to the limitations placed on the business and the users.
- CT5: The cost of adopting secured-by-design strategy while designing network infrastructure, configuration of operating systems and databases, or application development.
- CT6: The financial cost of items, equipment, facilities, or systems in order to recover from a security incident / threat.
- CT: The losses due to business interruption.
- CT8: The losses in human casualties or injuries.
- CT9: The losses in loss of data from business and legal aspects.
- CTIO: The losses in the reputation and goodwill.
- CTI1: The amount that the insurance pays due to the loss caused during an incident.
- KT: The probability of the security incident/breach to happen (without implementing any security control system I solution).

One of the difficulties in ROSI is to estimate values. CT1, CT2, CT3, CT5, CT6, CT7, CT8 and CT11 may be obtained or calculated from market prices, payroll and benefits, price schedules, security policies or historical financial data. CT4, CT9, CT10 and KT can be deduced from information security, consumer satisfaction surveys, surveys for advice or reports made by employees. Given these values, ROSI can be calculated over all security controls in (5):

ROSI= E [KT . (CT6 + CT7 + CT8 + CT9 + CTIO) + CTI I-(CTI + CT + CT3 + CT4 + CTS)] (5)

Where T value refers to the type of risk that the security control or system is exposed (intrusion, industrial espionage, DoS, information theft, malicious code, etc.). Although, (Al-Humaigani et al, 2003) approach risks to express ROSI, there are no considerations regarding RM frameworks extended to the ROSI analysis.

3.6 Evaluating ROSI using game theory

(Cavusoglu, et al 2004) advocates about a comprehensive and analytical model to evaluate security investment decisions considering the: 1) analyzes of individual security technologies used in the layers of the security infrastructure, which allows managers to assess the interaction among different security tools, as well as the use of this technology in ROSI; 2) conception of a target for deciding priorities for investment in technologies; 3) users decision for selecting and optimizing settings for security technologies, in addition allowing developers to design and evaluate security systems.

The proposed model does not act directly on the employed technologies, as it is not possible to assess how firewalls' vulnerabilities affect the expectation of losses. However, the model allows comparisons between different layers of IT security infrastructure. According to (Cavusoglu, et al 2004), one of the goals of IT security infrastructure is to reduce the risk to a point where the marginal cost of implementing controls is equal to additional gains coming from security incidents. The IT security infrastructure should be appropriate in order to

provide a plan for ensuring confidentiality, integrity and availability of information resources. Such plan consists of: 1) Risk assessment to determine the level of security risks in the organization; 2) Quantitative risk analysis concerned with the values of risk, as costs of potential damages and cost-effectiveness of security controls.

IT architectures should consist of several layers, with various security controls which are complementary to each other. The values of the controls are different and are also dependent on each other on each level. This requires a design that acts simultaneously on all layers. The model of (Cavusoglu, et al 2004) proposes creation of three layers: 1) Preventive layer: where firewall acts; 2) Detection layer: where IDS acts; 3) Answer layer: composed by manual monitoring.

With the creation of infrastructure in layers, the model uses game theory to analyze strategic decisions on security. Game theory is used to analyze problems in which the outcome of a situation depends on the strategy used by players. Regarding the ROSI issue, both organizations and hackers are players; the organizations' decision making processes for whether approving or not a ROSI depends on the amount of cyber attacks. Analogously, cyber attacks to succeed depend on the implemented security controls in the company. Fig. 8 illustrates the game tree, which is based on infrastructure layer, created by (Cavusoglu, et al 2004) to demonstrate its model to evaluate ROSI:

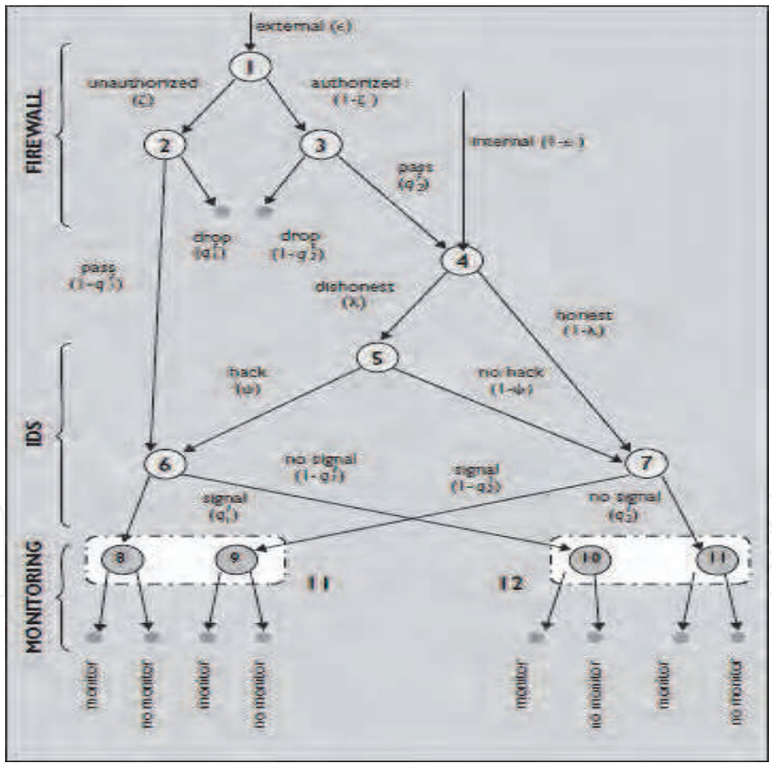

Fig. 8. The game tree

Items of Fig. 8 are:

- node 1 – receives external traffic;
- node 2 – receives unauthorized traffic;
- node 3 – receives external traffic allowed;

- node 4 - receives traffic internal and external authorized;
- node 5 - featuring authorized access to an internal network;
- node 6 - gets unauthorized access to external and internal users;
- node 7 - gets authorized access to external and internal users;
- d: expected damage to a security breach;
- ε: external traffic;
- (1-ε): internal traffic;
- ζ: external traffic unauthorized that can be blocked by firewalls;
- qF / 1: Probability of the firewall to stop unwanted traffic;
- (1-qF / 1): probability that the firewall does not stop unwanted traffic;
- qF / 2: probability of the firewall to pass traffic you want;
- (1-qF / 2): probability that the firewall does not pass the desired traffic;
- σ: cost that occurs when the unwanted traffic is caught by the firewall;
- λ: honests Internet users;
- (1-λ): dishonests Internet users:
- μ: fraction of dishonest users who gained access to the system;
- (1-μ): fraction of dishonest users who did not gain access to the system;
- qI/1: probability of the IDS to signal a malicious operation coming of μ or coming of (1-qF/1);
- (1-qI/1: probability of the IDS does not signal a malicious operation coming of μ or coming of (1-qF/1);
- c: cost that occurs when the monitoring layer indicates a possible intrusion;
- a: probability of the IDS detects a real threat due to the imperfection of monitoring;
- φ: fraction of the damages recovered when the intruder is detected by manual monitoring;
- β: fixed cost of an intrusion or malicious event;
- yd: cost of an intrusion (variable value proportional to the harm caused);
- p1: when there is a signal coming from the IDS;
- p2: when there is no signal coming from the IDS;
- Fs: expected results when there is a signal coming from the IDS;
- Fn: expected outcomes when there is no signal coming from the IDS;

With the use of (Cavusoglu, et al 2004)'s model it is possible for the organizations to make decisions about what to monitor (nodes 8 to 11) according to the status (named sign) of the analyzed traffic in the game tree. Using Bayesian rules, the company can determine the probability of intrusion when there is and when there is no signal coming from IDS.

The maximization of the company's expectations can be given by (6), (7) and (8):

$$F = [P(signal)FS + P(nosignal)FN + P(drop)\sigma] \quad (6)$$

$$\text{Where } FS = \{-\rho 1c - \eta 1(1 - \rho 1)d - \eta 1\rho 1[(1 - \alpha)d + \alpha(1 - \varphi)d]\} \quad (7)$$

$$\text{Where } FN = \{-\rho 2c - \eta 2(1 - \rho 2)d - \eta 2\rho 2[(1 - \alpha)d + \alpha(1 - \varphi)d]\} \quad (8)$$

The maximization of the hacker's expectations can be given by (10):

$$H = P(hacking)(Benefit - Cost) = \psi\mu - \psi\alpha(\beta + \gamma d)[\rho 1q1\,I + \rho 2(1 - q1I)] \quad (9)$$

Therefore, the proposed model is useful for some aspects of ROSI: 1) it helps to understand different parameters which affect the investment in security, as it is possible to simulate values in the game tree; 2) security controls can always be customized or configured. The process of setting changes parameters of quality, which influences the gains accounted in global security; 3) allows the choice of specific security technology. For instance, we can simulate the model as follows: step 1 – to select security technologies for deployment consideration, step 2 – to collect data about quality parameters q1I, q2I, q1F, Q2F, and costs of the concerning technologies, step 3 – to estimate cyber attacks and firm specific parameters such as d, γ, λ, φ, ε, σ, c, μ, α, and β, step 4 - to run the model for each security control and to determine the cost savings and step 5 - to choose the technology that yields the maximum savings.
Even though (Cavusoglu, et al 2004) recommends a previous RA before applying the ROSI model, RM frameworks are not approached

3.7 Forecasting for ROSI – Institute for technological research of São Paulo

As far as our knowledge extends, ROSI with forecasting was first applied by (Pontes et al, 2009a, 2009b, 2009c, 2010), which implemented a hybrid forecasting methodology combined with the cost-model of (Wei et al, 2001) for cyber attacks in the Internet. Fig. 9 shows the forecasting for ROSI, which generates two charts with two techniques (Fibonacci sequence and moving averages).

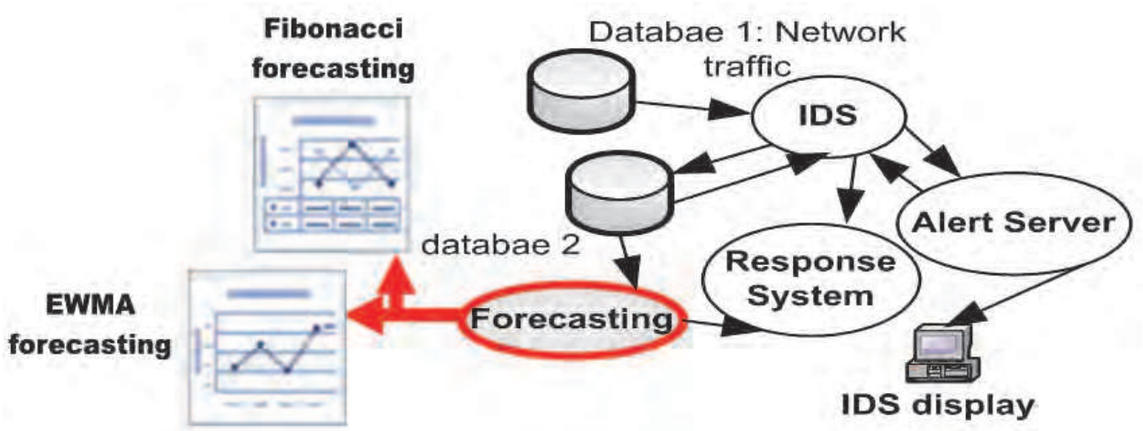

Fig. 9. Forecasting Methodology and Forecasting Generated Charts

(Pontes et al, 2009a, 2009b) used the datasets of (DARPA, 2009) representing the network traffic and an IDS (Snort, 2009) as a tool to analyze the network traffic. All security incidents (the intrusions attempts, alerts and logs) were lately recorded in another database. ROSI with forecasting collects the data from the second database; analyzes the information and then creates the trend charts, in accordance with the adopted techniques (Fibonacci sequence and moving average). However, in (Pontes et al, 2009a, 2009b) the forecasting for ROSI didn't approach three major gaps in forecasting techniques for IS: a) the use of few sensors and/or sensors employed locally; b) the use of just one forecasting technique; and c) lack of information sharing among sensors to be used for correlation.
Intending to improve the previous works, the goal of (Pontes et al, 2009c, 2010) was to propose the Distributed Intrusion Forecasting System Architecture (DIFSA) with prediction approaches and sensors acting in different network levels (host, border and backbone),

which enables the use of different forecasting techniques, the cooperation among points of analysis and the correlation of predictions. As results it was possible to increase reliability of attack predictions, to prevent attacks in a proactive manner and to improve RM employed for defense of the homeland cyberspace. (Pontes et al, 2009c, 2010) applied the DIFSA for sites geographically divided, with both usual and simulated traffic for normal and malicious activities (cyber attacks). Fig. 10 depicts the DIFSA and the forecasting levels.

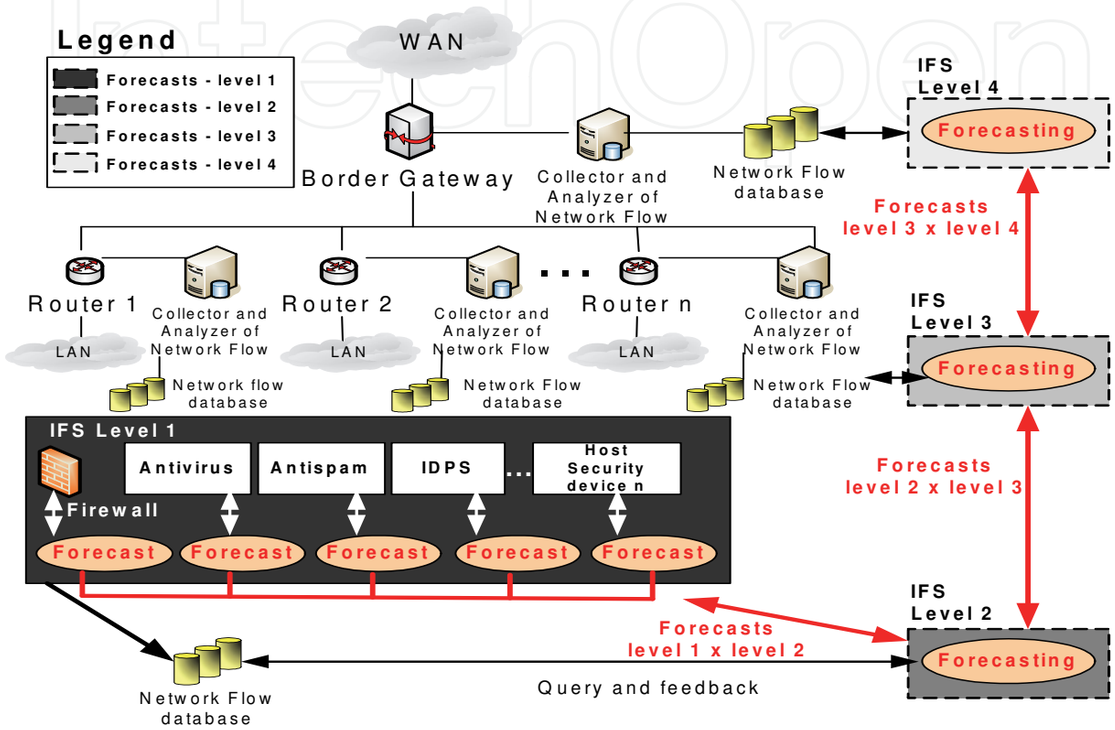

Fig. 10. IFS Architecture

Similarly to forecasting methodologies used in other fields, DIFSA also spreads agents and/or sensors widely to make predictions about the different kinds of cyber attacks. There are four levels of the IFS: level 1 - independent security devices of hosts; level 2 - integrated security devices of hosts; level 3 - the network level; and level 4 - the backbone level. All levels have some communication degree among each other. In other words, the forecasts obtained from level 1 are shared and correlated to the forecasts of the other levels. Lower levels work as sensors to higher levels; consequently feedback about the cyber attacks trends may be exchanged from one level to another.

Other prediction methods that may be employed with ROSI concern programming techniques, Markov chain, Fractal Analysis, stochastic processes, data mining, among others (Haslum et al, 2008). (Pontes et al, 2009a, 2009b, 2009c, 2010) did not approach RM frameworks in their works.

4. The comprehensive risk management framework

We hereby classify the comprehensive framework as the one which concerns each of the fundamentals of the traditional RM frameworks and, additionally, implements purposely a

ROSI phase. The comprehensive RM framework is composed of 5 phases and diverse steps, as Fig. 11 illustrates. The phases are:

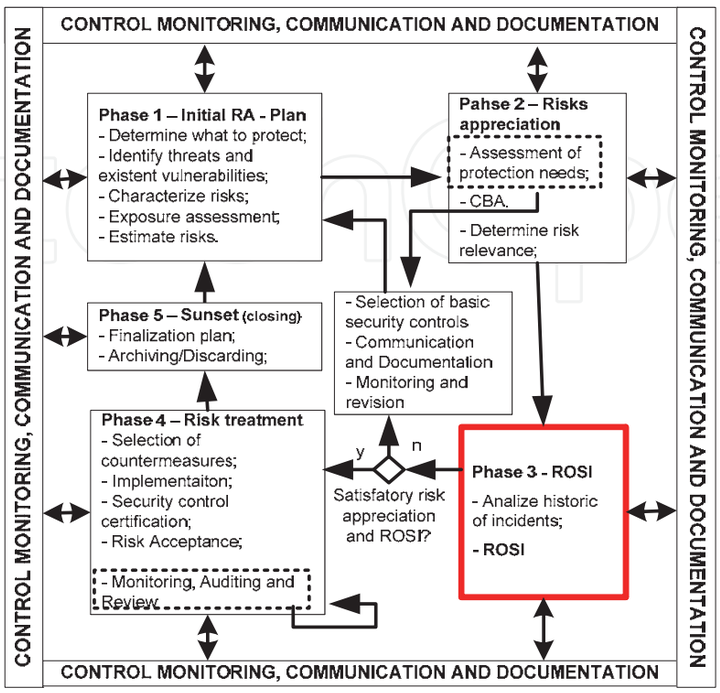

Fig. 11. The Comprehensive RM Framework – Extension to ROSI

Phase 1 – Initial RA: in this phase it is designed the plan for conducting the management activities, as defining scope for the RM environment (detailed description of the context and boundaries), defining the purpose of the RM. In addition, the first steps for RA are in this phase (threats identification, vulnerability analysis, assets identification, estimative about risk and the assessment of the exposure level for the assets);
Phase 2 – Risk appreciation: specific security requirements for organizations are defined in this phase, assessing and analyzing the protection needs by the use of CBA methods, estimating the ALE and the likelihood of the threats that may explore vulnerabilities;
Phase 3 – ROSI: this phase regards the analysis of the incidents history, adding 1) deeper financial analysis phase in the selection of controls, incorporating criteria such as loss of productivity, business organizational interruption, loss of intangible assets, depreciation, devaluation, reconstruction, recovery, monitoring of investment compensation; 2) evaluating security planning and security solutions, 3) analyzing business needs and security controls to be employed, 4) presenting the lowest possible values to address costs of security breaches and costs of security controls;
Phase 4 – Risk treatment: this phase concerns the selection of safeguards, as well as the implementation of countermeasures, certification of IS controls and the risk acceptance.
Phase 5 – Sunset (closing): phase performed to finalize all activities across the RM. This phase considers the hypothetical situation for transferring responsibilities, as archiving and/or discarding confidential information regarding third parties.
Phase 5 may happen whether for organization merging or when the activities of an organization come to end.

The comprehensive RM framework illustrated by Fig. 11 is cyclic, but in some phases the cycle may be interrupted, returning to the first phase. Because of the dynamic nature of risks, threats and vulnerabilities (GCIO, 2004), (ISO 31000, 2009), monitoring and communication plans must be described, defining the stakeholders (involved parties), as their roles and responsibilities properly delimited. As well as the countermeasures and risks' monitoring, communication and documentation must be constant during the entire RM, allowing each one of the stakeholders to know the progress of every processes and to provide subsidy for developing RM.

Phase 1 derives from (PMBOK, 2008), as it refers plan conception for conducting RM. However, in this phase there is extension to (FISMA, 2002), (ISO 27005, 2008), (NIST SP800-30, 2002), as the scope identification, context and boundaries definition, identification of assets, threats and vulnerabilities, assessment of the exposure and risks estimative.

During phase 2, after assessing the protection requirements, it is possible to identify imminent risks with potential impacts and, therefore, the need of risk treatment with immediate countermeasures implementation. At this moment, it is suggested interruption of the RM cycle, remitting to the selection of tailored baseline security controls to mitigate risks, followed by documentation and communication and lastly by monitoring and revision of the implemented controls and/or other security controls to be implemented.

In organizations which RM is executed for the first time, it is usual the cycle to be interrupted during phase 2, like the implementation of basic security controls (ISO 13335, 2004). Although CBA and ROSI are essential for IS controls selection, at this moment the priority is to protect the organizational assets which might be at serious risk, as it was previously appointed by the first phase of RM and by the assessment of protection needs. Phase 2 is analogous to the risk assessment of 27005, as procedures for the protection requirements; the risks level determination and ACB are performed.

Phase 3, ROSI, represents the main proposed extension for RM. In this phase the risk assessment previously performed is complemented by tracking and predicting the incidents flow for the near future. In the case the risk assessment or ROSI had not been satisfactory, because of lack of related data, the cycle will be redirected to the first phase again. In this case, it is essential to select basic IS controls, to communicate and document, monitoring and revision of existing controls. Otherwise, in the case ROSI and risk assessment had been successfully concluded, phase 4 will be initiated. In the comprehensive RM framework, ROSI approaches the analysis of historical series of incidents that were problem to productivity rates (Sonnenreich et al, 2006). ROSI concerns also the cost avoidance resulting from resistance, recognition, and reconstitution efforts for the IT infrastructure in the organization, based on the ALE and the number of incidents (Wei et al, 2001), (GCIO, 2004), (O'Neil, 2007); 2) ROSI may also include techniques to identify incident trends (Pontes et al, 2009a, 2009b, 2009c, 2010). Phase 4, risk treatment, is the moment for minimizing risks, selecting effective controls, implementing, accepting risks and certifying IS countermeasures (FISMA, 2002), (NIST SP800-30, 2002). Phase 4 considers options for risk reduction, risks retention, risk avoidance and risk transferring.

Although the control monitoring is constant during the proposed model, in this phase the process is complemented by auditing and control revision. Eventually auditing and/or revision may indicate that the implemented controls are not enough, and then phase 4 is restarted, but preceded of communication and documentation. When the IS controls correspond the audit requirements phase 5, sunset, is initiated. Phase 5 is aligned to the SDLC (System Development Life Cycle) (NIST SP800-21, 2005) and it contemplates the

hypothesis of finalization (extinction) or transposition or RM environment (e.g. organization merging) with archiving and/or discarding. Even though phase 5 is occasional, closing procedure is recommended to be planed, as follows:
Transposition: it happens during merging process of organizations, for instance. In this context, it is necessary to plan the closing, archiving and transfer process of RM. Documentation and communication are essential in this phase, as well controls monitoring. Phase 1 is retaken when transfer is concluded; Finalization: it happens when a company is closed. As RM is generally linked to third parties (governmental, private organizations), information disposal concerns treatment of sensitive data, as confidential information. Phase 1 is not retaken after closing.
Notice that the comprehensive framework is based on characteristics of other RM models, but ROSI with introduces an important increment for decision making process (Pontes et al, 2009a, 2009b, 2009c, 2010).

5. Analysis of ROSI application in risk management (RM)

Within the traditional RM (i. e., the one that deals with threats, vulnerabilities, probability of adverse events, impacts, risks and security controls for handling risks) the inclusion of ROSI provides a more discerning evaluation for selecting and acquiring IS controls in IT. The discerning evaluation is mainly due to the following factors:

- A ROSI approach in risk management (RM) adds a deeper financial analysis phase in selecting the most appropriate security control to address a specific risk, incorporating not only criteria of the technological feasibility and costs of acquisition, but also other touchstones such as loss of productivity, business organizational interruption, loss of intangible assets, depreciation, devaluation, reconstruction efforts, recovery efforts, monitoring of investment compensation in a control by minimizing or eliminating losses etc. Thus, a ROSI approach deepens and complements a cost/benefit analysis made in a RM, providing a more wide and appropriate evaluation of a given security control to be applied;
- Monitoring the investment compensation, regarding IS controls, is important for having a real perspective about the expected time for a given control to compensate its investments, by eliminating or minimizing losses which could occur if the control was not applied. Therefore, by the applied IS control, it is possible to keep the workability of business in order to make profit. Investment compensation in a given IS control can be understood as the savings generated by the protection of the business;
- ROSI approach in RM for IT enhances investments savings, as more efficient controls are required to protect and maintain the business of organizations;
- By the use of cyclic RM framework all together with the definition and collection of measures (metrics) associated with the applied controls in a given system, it is possible to reach the continuous improvement of these controls in a system, and it is also possible to verify whether the planning done for a given control will be fulfill or will require adjustments to its complete execution.

Notwithstanding, including ROSI approach in RM may also come out with some shortcomings. The first limitation is that the ROSI for an IT environment will always deal with the minimization or elimination of financial losses through the use and maintenance of one or more IS controls, thus generating savings. However, revenue or dividends are not

generated over the invested financial value. This is the limit that a ROSI approach provides to an organization.

The second shortcoming: ROSI approach will always generate an additional work phase on the traditional RM framework, thus making this model more complex and quantitative. Consequently, it is common to observe that, not only the ROSI approach, but often also the cost/benefit analysis, may simply be ignored in the RM process when critical or high risk issues are identified.

The third shortcoming: ROSI approach for deploying an IS control is based on events or incidents which have occurred in the past, or on the notion of the current protection level for an IT environment. Therefore, when deploying an adequate IS control at a given moment, it is not possible to assess the future trend of the attacks to see whether the investment compensation can occur for the short, medium or long term. That is, a ROSI approach can only wait for the real behavior of the next attacks to see whether the planning for investment compensation in IS controls was anticipated, fulfilled or postponed. In addition, the ROSI approach addresses the description of costs to avoid problems of IS in IT, regarding losses or damages estimated at a given time.

Finally, the traditional RM in IT can produce a reduced amount of satisfactory results when financial criteria is not evaluated in depth for the selection and implementation of appropriate IS controls. However, ROSI should not be applied individually for the IS controls selection process; ROSI should always be placed within cyclical RM framework, as controls can be better justified, monitored and periodically evaluated to generate larger savings in business.

6. Conclusion

As a conclusion this study has investigated some of the RM standards and good practices, proposing an extension to those common RM frameworks: RM with ROSI and the closing phase for RM. The implementation of the proposed framework is simple and easy to interpret. Our discussions indicate that such a framework is practical for protecting assets, which are at risks, prone to threats or misuse

Within the context of RM in information security, it is important 1) to define the risk levels, select and implement appropriate security controls; 2 it is also important to justify costs and investments and monitoring processes when such investments will be compensated by the prevention of losses and damages. In this reasoning line, the goal of this chapter was to propose a RM framework more comprehensive than the traditional ones, deepening the importance of using ROSI as a way to monitor and measure the compensation of fulfilled investments in security controls.

As mentioned in section 2, several traditional RM approaches, such as the ISO/IEC 27000 family, AS / NZS 4360, NIST SP 800-30, among others, deal more clearly with the risk identification and analysis, risk treatment, CBA, monitoring and reviewing of implemented controls. However, the traditional RM approaches refer furthermost to ROSI in a secondary and superficial way within their texts. Then, section 3 discussed a number of proposals made to calculate the ROSI associated with security controls in IT. The works done by (Sonnenreich et al, 2006), (Wei et al, 2001), (O'Neil, 2007), (GCIO, 2004), and (Al-Humaigani et al, 2003) have two characteristics in common: a) the ROSI calculations are always based on savings (loss prevention) and on investment value for a given control; and b) the ROSI calculations should take into account not only the values of fulfilled investments, but also the values related to the maintenance of the implemented control.

In the sequence, to meet the goal of the chapter, section 4 presented as proposal a comprehensive RM framework, extending the traditional approaches in two phases clearly stated: planning and monitoring of ROSI (phase 3); and closing or extinction of the IT environment resulting in the archiving or discarding activities within the system (Phase 5 - aligned to the SDLC addressed in NIST SP 800-21 (NIST SP800-21, 2005)). Finally, section 5 has shown an analysis of ROSI application in RM, including:

- Key Benefits:
- ROSI adds a deeper financial analysis phase in the selection of controls, incorporating criteria such as loss of productivity, business organizational interruption, loss of intangible assets, depreciation, devaluation, reconstruction, recovery, monitoring of investment compensation in a control etc;
- ROSI allows to potentiate the saving of investments and cost-effectiveness for the controls;
- With the collection of measures (metrics) associated with the controls, it is possible to verify if the planning done for a given control will be fulfill or not;
- Major limitations:
- ROSI generates savings, but neither revenue nor dividends arise from the invested financial value;
- ROSI brings up an additional work phase on the traditional risk management model, therefore making this framework more complex and quantitative;
- ROSI is based on events or incidents have occurred in the past or on the notion of the current protection level for an IT environment, thus it is not possible to assess the future trend of the attacks to verify if the investment compensation can occur in the short, medium or long term.

The following future works may be suggested: an experimental analysis of ROSI approaches applied in IT environments; to use forecasting techniques to know the behavior and volume of the security attacks, thus helping to verify if the planning done for the ROSI will be confirmed before or after the defined deadline; to prepare a formal proposal for the implementation of ROSI taking into account the life cycle of IT systems; among others.

7. References

Al-Humaigani, M.; Dunn, D.B., A model of Return on Investment for Information Systems Security, *Proceeding of 2003 IEEE International Symposium on Micro-NanoMechatronics and Human Science*, pp. 483, ISBN 0-7803-8294-3, Cairo, 2003.

Cavusoglu, H., Mishra, B., Raghunathan, S., A Model of Return on Investment for Information Systems Security, (2004), *Journal Communications of the ACM*, Volume 47 Issue 7, July 2004, ACM New York, NY, USA.

DARPA, Defense Advanced Research Projects Agency, DARPA, (1998), Massachusetts Institute of Technology (MIT) - Lincoln Laboratory, 1998, Available from http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/index.html.

Haslum, K, Abraham, A., Knapskog, S., Fuzzy Online Risk Assessment for Distributed Intrusion Prediction and Prevention Systems, *Proceedings of IEEE UKSIM 2008 10th International Conference on Computer Modeling and Simulation*, pp. 216, ISBN 0-7695-3114-8, Cambridge, UK, April 2008.

IC3 - Internet Crime Complaint Center, (2008), 2008 Internet Crime Report, Bureau of Justice Assistance and National White Collar Crime Center, 2008, Available from: www.ic3.org.

ISO 13335, International Standardization Organization, ISO/IEC TR 13335. Information Technology – Guidelines for the management of IT Security – part 1: Concepts and Models for IT Security, Geneva, 2004.

ISO 27001, International Standardization Organization, ISO/IEC 27001. Information technology -- Security techniques -- Specification for an Information Security Management System, Geneva, 2006.

ISO 27002, International Standardization Organization, ISO/IEC 27002. Information technology -- Security techniques -- Code of Practice for Information Security Management, Geneva, 2005.

ISO 27005, International Standardization Organization, ISO/IEC 27005. Information technology -- Security techniques -- Information security risk management, Geneva, 2008.

ISO 31000, International Standardization Organization, ISO/IEC 31000. Risk management — Guidelines on principles and implementation of risk management, Geneva, 2009.

ISO 73, International Standardization Organization, ISO/IEC Guide 73. Risk management Risk Management Vocabulary, Geneva, 2009, Geneva, 2009.

NIST SP800-21, National Institute of Standards and Technology, (2005), Guideline to Implement Cryptograph in the Federal Government, USA, 2005.

NIST SP 800-30, National Institute of Standards and Technology, (2002), Risk Management Guide for Information Technology Systems, USA. 2002

NIST SP 800-37, National Institute of Standards and Technology, (2010), Guide for Applying the Risk Management Framework to Federal Information Systems, USA, 2010

PMBOK, Project Management Institute, (2008), PMBOK – Project Management Body of Knowledge, A Guide to the Project Management Body of Knowledge, Forth Edition, Paperback, PMI, December, 2008.

Pontes, E. & Geulfi, A., (2009), IDS 3G - Third Generation for Intrusion Detection: Applying Forecasts and ROSI to Cope With Unwanted Traffic, *Proceedings of 2009 4th IEEE ICITST International Conference for Internet Technology and Secured Transactions*, pp. 1, ISBN 978-1-4244-5647-5, London, UK, November 2009.

Pontes, E. & Guelfi, IFS — Intrusion Forecasting System Based on Collaborative Architecture, *Proceedings of 2009 4th IEEE ICDIM International Conference on Digital Information Management*, pp. 1-8, ISBN 978-1-4244-4253-9, University of Michigan, Ann Arbor, USA, November 2009.

Pontes, E. & Zucchi, W., (2010) Fibonacci Sequence and EWMA for Intrusion Forecasting System, *Proceedings of 2010 5th IEEE ICDIM International Conference on Digital Information Management*, pp. 404-412, ISBN 978-1-4244-7572-8, Lakehead University, Thunder Bay, Ontario, Canada, July 2010.

Pontes, E., Guelfi, A. & Alonso, E., (2009), Forecasting for Return on Security Information Investment: New Approach on Trends in Intrusion Detection and Unwanted Traffic, *Journal IEEE Latin America Transactions*, Vol. 7, Issue 4, (December 2009), pp. 438-446, ISSN 1548-0992, São Paulo, Brazil.

SNORT, 2009, Available from http://www.snort.org.

United States Government, (2002), Federal Information Security Management Act of 2002 - FISMA, USA, Dec. 2002, Available from: http://csrc.nist.gov/groups/SMA/fisma.

W. Sonnenreich, , J. Albanese, and B. Stout, (2006), A practical approach to return on security investment, *Journal of Research and Practice in Information Technology*, Vol. 38, No. 1, pp. 45-56, ISSN 1443-458X, Australia, February 2006.

Risk Management in Environment, Production and Economy
Edited by Dr. Matteo Savino

ISBN 978-953-307-313-2
Hard cover, 214 pages
Publisher InTech
Published online 12, September, 2011
Published in print edition September, 2011

The term "risk" is very often associated with negative meanings. However, in most cases, many opportunities can present themselves to deal with the events and to develop new solutions which can convert a possible danger to an unforeseen, positive event. This book is a structured collection of papers dealing with the subject and stressing the importance of a relevant issue such as risk management. The aim is to present the problem in various fields of application of risk management theories, highlighting the approaches which can be found in literature.

How to reference
In order to correctly reference this scholarly work, feel free to copy and paste the following:

Elvis Pontes, Adilson E. Guelfi, Anderson A. A. Silva and Sérgio T. Kofuji (2011). A Comprehensive Risk Management Framework for Approaching the Return on Security Investment (ROSI), Risk Management in Environment, Production and Economy, Dr. Matteo Savino (Ed.), ISBN: 978-953-307-313-2, InTech, Available from: http://www.intechopen.com/books/risk-management-in-environment-production-and-economy/a-comprehensive-risk-management-framework-for-approaching-the-return-on-security-investment-rosi-

INTECH
open science | open minds

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