THE PATTERNS FOR INFORMATION SYSTEM SECURITY

Diego Abbo
School of Systems Engineering, University of Reading, U.K.

Lily Sun
Director of Postgraduate Studies, School of Systems Engineering, University of Reading, U.K.

Keywords: Security applicative models.

Abstract: The territory of IS is continuously improving its capacities, new architectures grow at a brisk pace and qualitatively the functional processes are deepening the degree of interaction inherent in the services provided.

In the logical and/or physical territory of application, security management wisely faces the inherent problems in the domains of prevention, emergency and forensic investigation.

If the visionary plans are good the security breakages will be going to be within the "residual risk profiles" of a congruous preventive risk analysis, and any further business development will match costs of security safeguards with the detrimental economical consequences of security breakages.

In that perspective the IS security should have a larger field of application than the traditional security vision in the sense that the mere responsibility of a security domain should not only consider the immediate self interest of the owner of the asset.

The IS security should consider the horizontal and hierarchical integrations and interoperability with all the correlated security systems or all the security needed systems, with an intrinsic capacity of evaluation any possible future model.

The most efficient security should results the one that can individuate all the possible variables that constitute the basic for the patterns.

1 INTRODUCTION

The patterns for IS security is a proposed approach perspective, completely engaged in the broadest IS architectures. It aims to create a conceptual reference lay-out in order to adapt, extend or change the conventional IS security issues in accordance with models that consider exhaustively the actual and future requirements of e-society.

The main genre of security literature encompasses a two-headed framework. The first focuses the management of general security with the growing of rank importance in the corporate agenda. The second concerns the information security, its technological solutions and standard organized on best practiced behaviours.

The security management adopts a process approach for establishing, implementing, operating, monitoring reviewing, maintaining and improving an organization's Information Security Management System (ISMS).

The principal aim of this paper is to introduce new horizons of research in order to fulfil actual and future security pattern analysis .

In second instance it would like to individuate new "food for thoughts" in order to define properly security models an patterns.

This manuscript is organized as follows: firstly it outlines the conceptual references of security and its management.

Secondly it focuses how security performs in accordance with the quantity of dedicated resources and the quality of the reactive defence profile.

The conclusion wants to address the future analytical paths for a better IS security.

Abbo D. and Sun L. (2009).
THE PATTERNS FOR INFORMATION SYSTEM SECURITY.
In *Proceedings of the 11th International Conference on Enterprise Information Systems - Information Systems Analysis and Specification*, pages 342-346
DOI: 10.5220/0001953003420346

2 THE PATTERNS BUILD-UP

2.1 The Actual Scope

The first achievement that the management of information security outlined was the key characteristic of information that make it valuable to an organisation.

The C.I.A. triangle (Confidentiality, Integrity, Availability) has been industry standard for computer security since the development of the mainframe.

The components of the C.I.A. were defined as follows (E-Government Act of 2002):

"*Confidentiality, the preservation of authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information;*
Integrity, guarding against improper information modification or destruction, which includes ensuring information non repudiation and authenticity;
Availability The property of ensuring timely and reliable access to and use of information."

Threats to these three characteristics of information have evolved into a vast collection of potential danger, including accidental or intentional damage, destruction, theft, unintended or unauthorized modification, or the misuses from human or other threats (WHITMAN p. 6)

The new environment of constantly evolving threats has necessitated the development of a more robust model of the characteristic of information. The C.I.A triangle has expanded into a more critical list of information: privacy, identification, authentication, authorization.

The concept of computer security has been replaced by the concept of information security that is achieved via many routes, with several approaches usually undertaken singly or used in combination with one another.

Furthermore the approaches should be integrated with the specialize areas of security include the following: physical security, personal security, operations security, communications and network security.

From a managerial perspective each must be properly planned, organized, staffed, directed and controlled.

Organizations have the option of performing a risk assessment in one or two ways: qualitatively or quantitatively. Qualitative risk assessment produce valid results that are descriptive versus measurable.

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.

In that case the definition of risk, is assumed as "*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*." (ISO/IEC Guide 73, p. 2)

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.

However the increasing dependence of the human activities from the ISs make more and more difficult the estimation of a given risk by the traditional statistical and /or analytical model (RSSG p. 4).

The top edge of security management is represented by the International Standard, that has been prepared to provide a model for establishing,

implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISO/IEC 27001 p. v–vi).

The International Standard adopts the "Plan–Do-Check–Act" (PDCA) model which is applied to structure all ISMS process as it's shown in figure 1.

The frontiers in IS security management is to look at the organization itself and identify what needs to be protected, to determine what is the risk, and to develop solutions requiring both technology and practise based solutions.

The International standard is aligned with related management standards and represents a core reference for quality assurance auditors of Security Management.

However all the current methods of security management based on quantitative analysis of risk are "bottom up":

They start with the computing infrastructure and focuses on the technological vulnerabilities, without the non complete capacity of considering the risks to the organizations missions and business objective.

The first element of inadequacy should be individuated in the absence of a proper model that can fully describe the relationship between threats and countermeasures or in other words the performance of security in a given model. That means a pervasive analysis of the security breakages in order to redefine the risk parameters and to achieve a fully forensic capacity.

A second element is the lack of real time flexibility. The risk analysis is linked both to the internal issue of an organization, and to the external pertinent aspect.

The internal issues are supposed to be lasting whereas the external environment, overall the components that affect security, changes quickly and with short prevision.

Furthermore the last but not least element is the escalatory growing IS system interaction with human activities.

Actually the integration is moving towards an interaction within EXTRANETs'.

EXTRANET is defined as " *a secure network that uses the INTERNET and Web technologies to connect two or more INTRANETs of business partners enabling business-to-business, business-to-consumer, consumer-to-consumer, and consumer-to-business communications. Extranets are a network service that allows trusted business partners to secure access to useful information on another's organisation Intranet.* " (BIDGOLI p.9).

It is possible to integrate or make working business partners that are matching models with a different level of security.

The core aim is to create measurable model for IS system security exploiting the numeric nature of analysis. The aim is to achieve a twofold effect: in one side have the possibility of measurable confrontation between different levels of security. In the other side it should constitute an up dated feedback for any future quantitative risk analysis.

2.2 The Model Build-up

A formal model for IS security is a process for building into computer – based systems while exploiting the power of mathematical notation and proofs. A formal method relies on formal models to understand reality and subsequently implement the various components.

A model can be constructed as an abstraction of reality and a mental construction that is embodied into a piece of software or a computer based information system.

The release point is to consider, in any given organization, what is the "rate" of Information protection that can be implemented what is the corresponding running of security. That pattern can be achieve considering, in the given organisation, three interactive entities that we can consider linked by rules of a close market.

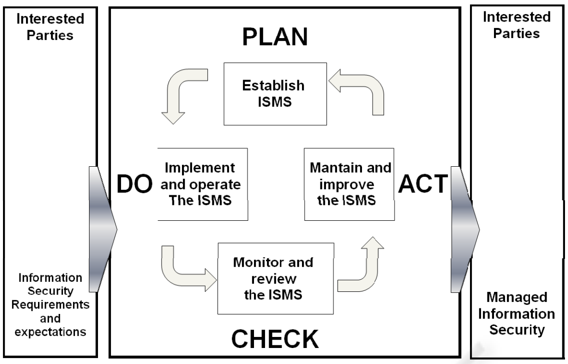
Interested Parties
PLAN
Establish ISMS
DO
Implement and operate The ISMS
Mantain and improve the ISMS
ACT
Monitor and review the ISMS
CHECK
Information Security Requirements and expectations
Interested Parties
Managed Information Security

Figure 1: PDCA model applied to ISMS processes.

The first entity is "IS 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 IS security missions and has supporting services as a feed-back.

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 fulfil its mission.

One of the key point that any instrumental item can have a multiple use one for each entity. For instance an employee is dedicating his working time to Company Mission" but he is spending a percent of this working time to "Information mission" for duty purposes (e.g. production of digital documents, connection with the network etc.). and smaller percent of time is dedicated at IS 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 IS security mission we have the "iso-line of balanced budget" (see figure 2).

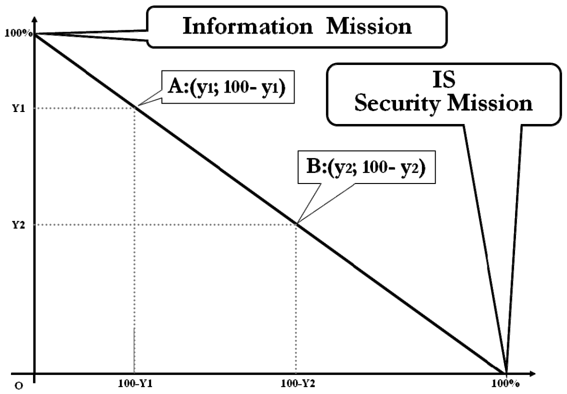

Figure 2: ISO-Line of balanced budget.

Having several class 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.

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 (figure 3).

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 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 represent the either the value of "threat performance" or the "quantitative risk analysis" for any model that has the same premises and surrounding conditions.

Actually 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.

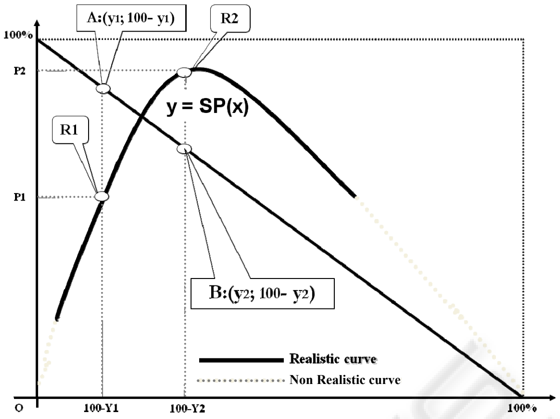

Figure 3: Curve of Security Performance.

However the interlocking sets, ideally assimilated to the links of the security chain, should follow the wise principle that "no chain is stronger than its weakest link". The "security chain model" runs in a mathematical model that creates a comparative scale between each single link in order to make-up a "flexible security thermometer" for the whole security chain fully understandable by stakeholders, users, security managers, system administrators etc.

In order to create the "flexible security thermometer" we proceed in the following way for each link of the security management chain:

to individuate an A-menu of all the possible up-to-date safeguards and resources we can apply to each single link;

to manage a shrinkage of the A-menu (that can be called best operational menu) after making a qualitative risk analysis where it has been considered in general terms the structural protection of the enlarged C.I.A. triangle, the functional costs, the estimated curve of security performance and the following mathematical inequality commonly called security equation:

$$Pt > At + It$$

That means the penetration time (Pt) should be larger than the sum of Alert time (At) and Intervention time (It) that need the security safeguards to neutralize the action of the Threat. If the equation is satisfied we are in the domain of prevention if not we are in the domain of emergency (for which we should follow the business continuity and/or disaster recovery plans) and subsequently in the domain of forensic investigation.

In that analysis we also define which safeguards are mandatory, which are not mandatory but normally implemented as best – practice, elective and which should be escalatory to be implemented in security contingency plans (either preventive plans or emergency plans) for a definite period of time. An important issue that should take into consideration is the ”watertight bulkhead capacity” of the data domain versus the interaction with other domains, beyond the security control of the owner.

The point is if the interaction can generate a possible further profile of vulnerabilities.

we draw a list of the safeguards shared in four classes (mandatory, best practice, elective, and on call); for each of those safeguards we associate a number (safeguard security coefficient) taking into consideration that the sum of all the safeguard security coefficients should equal 99;

we apply the following formula to each link of the chain, after individuating the “most suitable operational menu”:

$$LS = 1:(100- \alpha)$$

Where LS stays for “Link Strength” and α is the summation of the security coefficient of all the implemented safe-guards and it is a scalar quantity included between 0 and 1

$$0 < LS \leq 1$$

we multiply all the LS together and we obtain the CS “Chain Strength” that is another scalar quantity, considering n links, ranges from:

$$10^{-n} < CS \leq 1;$$

The CS and LS are pure numbers but can be used as a kind of industrial dashboard that is a very useful tool to compare, standardized, measured and in comparison with the graphic in figure to have in real time the ICT Security proficiency.

The application of The LS and CS quantities represent the percentage of the safeguards of the best operational menu that has been implemented.

The “security chain model” approach may trigger a great impact on IS security. Its numeric analysis is a potentially tremendous tool that provide an extreme range of flexibility and the total congruency with any related party to the ISs.

The only undetermined issue is how this model perform, but for that is necessary a trial stage from the IS communities.

3 CONCLUSIONS

The purpose of seeing the IS security models 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 analytical pattern approach is not only the possibility of always estimating costs, 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. This can be exposed if compared with features of the scientific approach to problem solving. The means that are characterizing the nature of inquiry are “experience”, “reasoning”, and “research” and those premises are the core advantage in applying a pattern design.

The possible applications are inclusive of all the IS architecture and a scientific analytical approach should became a must when entering in the top level stages

The limitations in the applications are mainly instrumental in the sense that in any security issue it should be considered its functional cost.

REFERENCES

Bidgoli, H., 2006. *Internet basics,* Handbook of Information Security Vol. I, Hossein Bidgoli Editor in Chief, John Wiley and Sons Inc., New Jersey.

E-Government Act of 2002. Title II, *Federal Information Security Management ACT (FISMA),* Pub. L. No. 107-347 (2002). Retrieved from http:// thomas.loc.gov/bss/d107/d107/laws.html.

ISO/IEC 27001, 2005. *Information technology – Security techniques – Information security management systems – Requirements* Milant 1st edition.

ISO/IEC GUIDE 73, 2002. *Risk management - vocabulary – guidelines for use in standards* Geneva 1st edition.

RSSG - Report of a Royal Society Study Group, 1992. *Risk analysis perception management,* The Royal Society – London.

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