Reasonable Security by Effective Risk Management Practices: From Theory to Practice

Solange GHERNOUTI-HÉLIE
Faculty of Business and Economics
University of Lausanne
sgh{@}unil.ch

David SIMMS
Faculty of Business and Economics
University of Lausanne
David.Simms{@}unil.ch

Igli TASHI
Faculty of Business and Economics
University of Lausanne
Igli.Tashi{@}unil.ch

Abstract

In this period of grave economic uncertainty, organizations have to manage increasingly complicated situations in an environment that is subject to massive and rapid evolution. A solely intuitive approach to risk management is no longer sufficient when considering the need to optimize investments in relation to security. It is necessary to find the often difficult balance between the cost of risks and their mitigation so as to ensure that organizations can realize their objectives in a reasonable and durable manner.

The aim of this paper is to demonstrate the strong need for information system owners and managers to rely upon an effective risk analysis methodology for decision making related to efficient security measures in order to enhance business performance.

We present a methodological approach. A case study and description of real-life experiences are presented in order to illustrate the applicability of this approach.

Keywords *— Uncertainty, Risk and Security Management, Information Systems and Security Governance, Information systems conformance issues, Sustainable development, Responsibility, Complexity Management, Multidisciplinary approach, Real life case study.*

1. Introduction

In this period of grave economic uncertainty, organizations have to manage increasingly complicated situations in an environment that is subject to massive and rapid evolution. A solely intuitive approach to risk management is no longer sufficient when considering the need to optimize investments concerning security. It is necessary to find the difficult balance between the cost of risks and their mitigation so as to ensure that organizations can realize their objectives in a reasonable and durable manner.

The current, turbulent state of the economic environment is partly due to an absence of appropriate and consistent risk management within businesses that aimed to generate increased profits while either ignoring risks or assuming that risks were under control.

The aim of this paper is to emphasize the role and value of information, the pertinence of decision–taking processes, and the implications of information technologies and good communications, in the overall framework of corporate and organizational governance and in the management of financial risks?

2. Information Systems Governance and Balance of Interests

There are many possible definitions of governance[1],[2], [3], [4], [5]; for the purposes of this paper we are using it to describe a mechanism that

978-0-7695-3767-2/09 $25.00 © 2009 IEEE
DOI 10.1109/NBiS.2009.66

allows us to take good decisions in the context of a more or less complex given environment. The tools associated with good governance are thus those that support the ability to take good decisions, in particular by implementing a system of efficient guidance.

The good governance of risk management allows us to master the difficulty of finding a judicious balance between the principles of elementary precautions and taking risks that can be evaluated, mitigated and managed, in an objective and systematic manner.

This approach will permit us to establish a well balanced framework to:

- Ensure continuity;
- Ensure flexibility, allowing rapid reaction to inevitable disturbances;
- Avoid the irreversible;
- Optimize performance;

having taken care to identify the characteristics of the different resources in question and the relative strategic values that have to be preserved.

The amount of protection a resource requires depends on the value that is assigned to it. This value can vary according to the players and its usage, and over time. The effort to be made in analyzing risk degradation depends on the assessed relative values of the resources.

In terms of protecting resources, one can, as an analogy, refer to the declaration from the Rio Summit [6] that reminds us that "it is necessary to limit, frame or avert those actions that are potentially dangerous, without waiting for the danger to be scientifically proven".

This sets out the foundation of the precautionary principle, which says it is preferable to avoid action when the consequences of that action could be major and irreversible and are impossible to predict with scientific certainty.

The principle of precaution specifically applies therefore to potentially grave but uncertain risks that threaten potentially irreversible consequences, especially when poorly identified. This brings us back to uncertainty, to the quality of the information and the decision-taking process, and to some questions:

- How to take decisions in a context of uncertainty?
- As of when does one consider that the knowledge available is uncertain, or on the contrary sufficiently certain?
- How to apply the precautionary principle? Sometimes this will be a matter of simple common sense, but caution must be exercised as a simplistic, overly cautious approach based on prudence could lead to ignoring alternative economic activities that would increase competitiveness?
- How to identify and describe the probability of a risk occurring, as well as the potential gains if avoided, when our knowledge is uncertain?
- How to evaluate the capacity to cover a risk, in insurance terms, so as to allow its reversal or financial compensation?
- How to distinguish between real dangers and those generated by fear? It can be a challenge to differentiate between real risks, fear, alarmist rumors or intellectual fraud, and for managers to identify reliable tools for taking good decisions, in a context of uncertainty.
- How to build the capability to manage great uncertainties – the inherent difficulty in all prevention exercises?

Even if in practice it is impossible to master all of these uncertainties, it is possible to evaluate their consequences, assuming that the effects of the evolution of the various exogenous (external) and endogenous (internal) parameters on the performance of the enterprise can be modelled.

Such a model must be simple and be based on a few key factors, but always built with the help of efficient governance. And, of course, this governance must not omit the principle of prevention.

3. The principle of prevention and risk opportunity strategies

The principle of prevention applies specifically when the risks can be clearly identified. It thus is a preventive measure, a question of attacking the problem at source rather than a post-hoc corrective measure.

Prevention can only really be implemented if our understanding of the existing mechanisms in place allows an accurate estimation of the damage and if proportional preventive action is possible [7], [8], [9].

It should also be remembered that prevention is encapsulated in the precautionary principle because it defines the totality of the tasks destined to avoid the given threats in the short term, or to limit and reduce the risk of impacts in the longer term. Hence it covers the adoption of effective measures to avert risks of serious and irreversible damages even in the absence of certainty.

Knowledge of the value of the resources is essential because it decides whether or not a preventive action is viable and thus drives all security actions.

The underlying principle is to reduce risks step by step, until the level is reached where every additional step will cost more than the discounted savings.

The best plan is useless if not acted upon and the feasibility of its implementation is as important as its objectives.

A significant factor that needs to be appropriately considered when addressing questions of security, risk, prevention and precaution is fear. Fear does not facilitate the success of a security plan and although it plays a largely underestimated key role, emotional reactions need to be avoided.

Notably, since the events of 11 September, we have experienced an increase in discussions about fear where risks are concerned, which are echoed in more general fears such as criminality, delinquency, bio-terrorism, and pandemics.

It is difficult to disassociate fear from real danger. It is, however, important to seize the ambivalence of fear, both a primitive emotion and a complex social characteristic. It is implied in a good number of behaviors: flight from real dangers, anxiety in the face of imaginary dangers.

Fear can lead to avoidance strategies which are entirely valid from a security point of view as awareness is raised. Calculation of the risk drives protective and preventive actions but can also, however, generate paralysis of the economic and social development of the enterprise or company.

As a disturbing but also a regulating factor, fear is not limited to a negativity that is largely uncontrollable, it works as a vector that pushes towards the need to find good tools, and helps in taking decisions based on maximum knowledge in spite of incertitude.

It should not be forgotten that in some contexts there exist advantages in orchestrating and instrumentalising fear, so that solutions are selected that are far from meeting the needs of those concerned.

Fear concerns the manager personally, with regard to his or her civil responsibilities as well as financial losses or the corporate loss of image.

On top of this we have to force ourselves to respond rationally and with discrimination. This brings us back to the importance of determining the value of assets, of our comprehension of the environment to be protected and the relationships between the entities of which it is composed that themselves command the dynamics of its operations, and thus the governance of the whole.

There is no universal solution that answers the specifics of each situation, the solution will depend, amongst other things, on:

- the collective mobilization of all the players; and
- the provision of a template that is simple, that integrates and consolidates.

The risk, up to now seen as a negative element to be suffered, tends to become an integrated element of contemporary society, as has been emphasized by Ulrich Beck in 1986, in his reference work “Society at Risk” [10].

This integration translates itself into an evolution of mentalities and behavior, using the mastering of risks as a requirement for greater security. Modern technologically advanced societies and their citizens no longer accept catastrophes as simple, unavoidable destiny (examples here would be nuclear accidents such as Chernobyl, chemical accidents such as AZF, or the construction of buildings that are not earthquake resistant).

This integration is also a general search for those responsible in times of crisis that ends up in demands for indemnification as soon as losses and damage are identified.

Furthermore, there exists today a common requirement for more and more security, while denying or downplaying the reality of uncertainty and risk. The requirement for maximal security is omnipresent.

Scientific and philosophical thinking of the past centuries allowed the belief that would be possible to attain absolute security, to efface uncertainty and to completely master risk. Today, computer systems, with their inherent complexity have allowed the re-invention of fear, with the distinction that it is not only nature that generates risks or major catastrophes, but also science and technology. We are far from the optimism of the 19th century.

Some technology-linked risks are all the more menacing for being global, due to the interdependence of our infrastructures [11]. They exceed the understanding of any given person or institution and demand a certain amount of cooperation between private and public players at both the local and international level, thus generating even more complexity to the governance of security.

The cultural evolution of the apprehension of risks is visible in its analysis and treatment, highlighting the diversity of our management methods that themselves closely depend on our knowledge and evaluation thereof. Risk also becomes an opportunity for economic development and a competitive factor, not only for the suppliers of information security solutions, but also for example for architects, for urban planners or civil engineering companies who try to counter the effects of a tsunami or potential earthquakes due to tectonic plate movement.

Thus, depending on the players and the framework of their intervention, the representation of risk takes on specific dimensions with socio-economic constructions, with the perception of an opportunity to bring progress, well-being, performance,

competitiveness and financial revenue. In brief, the management of opportunity risks.

We know of methodological, deterministic and probabilistic procedures that bring little information concerning the dangers over time of the management of complexity and incertitude. Some methods mix the empirical with expertise and do not necessarily allow good risk management and rarely provide reasonable security due to their immense complexity and the difficulty for management to interpret and use their results. This highlights the challenges of simplicity and the appropriation of expert knowledge for the corporate players.

Concretely the answer to good risk management is embedded in four main skills. With:

1. Engineering techniques and scientific skills,
2. Legislative and legal skills,
3. Governance and managerial skills,
4. Insurance skills ;

one will first try to determine, the amount of necessary risk that would be economically and socially acceptable. That is to say, the amount of risk to which one is prepared to be exposed, given the discounted advantages and the level of confidence in the evaluation and control methods.

Now is the time to mention the courage of some decision makers who take up the challenge of mastering risks and who take responsibility in an economic context where the performance pressures are exacerbated.

4. An analytical approach to risk management to obtain a reasonable level of security.

This approach is not a ready made recipe coming from a checklist, but rather a methodological framework that is sufficiently generalized and simple to be applied to all functions/professions/domains within an enterprise, while sufficiently detailed to allow an efficient analysis of the risks, to adequately determine the measures to be taken to treat them and to promote a culture of addressing risk within the heart of the enterprise.

This methodological framework has to be able to address all risks, whatever their nature (financial, environmental, operational, related to information technology and systems) in a uniform manner, integrated across all functions of the enterprise. The principal goal of such a method is to push organizations towards adopting a risk managing culture [12], [13] and it proposes objective methods to opt for a level of security that is neither too overwhelming nor too weak, to avoid an over investment in security, while ensuring sufficient protection. Thus it contributes to mastering the security budgets that the majority of relevant studies and analysts repeatedly predict will need increasing, without addressing the costs of the reasonably efficient and effective solutions implemented.

4.1 An integrated approach of risk and security aspects

First of all, ones can easily deduce that there are two main approaches to be performed in order to reach an assurance level regarding the safety of organizational values: a risk–based approach and a security–based one. These two approaches address the same overriding objective, the safety of the organization's valuable assets, but each one is driven from different mid-level objectives. Conceptually, the risk management process plays an ever-increasing role in security risk strategies [14], as it is the first input to the second stage which is effective Information Security. In order to achieve the goal of effectiveness in the domains of security and assurance, both approaches have to be integrated.

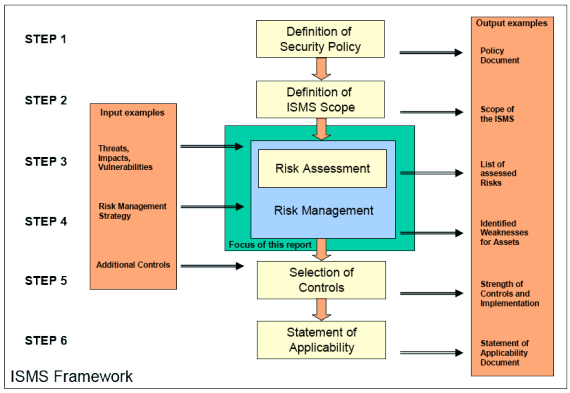

Figure 1: ISMS framework integrating both processes of Risk and Security Management

The aim of a Risk Management process is, generally speaking, to identify, evaluate and mitigate risks by choosing appropriate measures for protection [15], [16],[17].

The Information Security process supports this stage by making sure that the security measures in hand are correctly implemented, and they are not only effective but also efficient [18], [15], [19]. In fact, the Information Security process ensures that the protection measures are implemented in an appropriate and applicable way and that they are consistently and effectively applied. In addition, it is within the scope of

the Information Security process to ensure that every organizational, technical and human change is considered and the process is updated regularly.

Risk Management will outline the appropriate security controls to be operated. The security management ensures that the security controls are operated in the most effective and efficient way. Different and complementary competencies are clearly required to fulfill the requirements of both processes.

This method of proceeding will respond to the first requirement regarding the establishment of a reasonable security level. Starting with the Security Policy as shown in Figure 1 means that all security controls, procedures and activities will be driven by organizational objectives, stated within the policy, rather than by compliance standard claims. By the same deductive reasoning, the coherence criterion is also achieved.

4.2 Embracing a governance approach

To move further towards our final objective of reasonable security a governance approach, rather than a standard-based implementation approach is needed for multiple reasons.

Governance implies supervision and controlling operational activities, thereby placing the criterion of improvement in the core of the system. Governance is the process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that, information security strategies [1]:

- Are aligned with and support business objectives
- Are consistent with applicable laws and regulations through adherence to policies and internal controls
- Provide assignment of responsibility

The term Information Security Governance describes the process of how Information Security (IS) is addressed at an executive level [20].

In the context of the management of information systems and the implementation and maintenance of reasonable information security, governance in our model can be split down into four key objectives.

The first of these is continuity, ensuring that services can recover and continue should a serious incident occur. A key element of continuity is in ensuring that there is no loss of processing, so that should a restoration of services be required they are restored at the same status as before the loss of service – or that users are appropriately informed of the extent of the loss of processing and the actions to be undertaken to remediate the situation.

Secondly, resilience is the ability to provide and maintain an acceptable level of service in the face of errors, interruptions to communications and processing, and deviations from normal operations.

Thirdly, availability is the provision of access to functioning systems. Its definition and calculation in the IT context is often the subject of differing views between the IT and business functions, because a simple calculation of the uptime of a system, for example, may be numerically accurate but fail to reflect the fact that the single period of downtime occurred on the final day of the month, preventing the business from performing a number of key procedures.

Finally, management is concerned with optimizing performance. This can be less technical but a fundamental part of governance, seeking as it does to gain the maximum utility from the resources in place while managing costs and still enforcing appropriate controls over security and system management.

Governing IS security means that a given organization possesses:

- an IS risk management methodology
- an IS strategy
- an effective IS organizational structure
- some IS policies
- a complete set of security standards
- an institutionalized monitoring processes
- some process to ensure continued evaluation and update of security policies, standards, procedures and risks

In that way, the decision making process becomes more transparent, structured, and comprehensive, in order to better respond to the complex and polymorphic characteristics of risk.

4.3 Reaching an efficient guidance stage

As stated below the efficient guidance stage is function of two variables:

1. Standard precautions, which could be defined as a baseline security level, everybody has to implement.
2. Risk appetite appropriate to a given organization evolving in a given context under given objectives.

Reaching an efficient stage means thus gaining knowledge of the different standards, best practices or current practices in use. This is relation to the first variable but in practice cannot be considered to be

sufficient, as it might only allow the organization to achieve the same level of insecurity as others do.

Secondly, in order to define the risk appetite, a deep knowledge of security capabilities is required in order to be sure that we are taking risks we are proficient in managing. It implies a top-down understanding of the existing mechanisms and a whole view of the totality of tasks performed within the organizational perimeter.

This requires a formal analysis system guided by the general vision of the organization regarding opportunities, risks and security countermeasures.

4.4 Reasonable and durable security assurance

Such a formal analysis could be performed in the circumstances where an organization has already deployed a set of well-documented control objectives, controls and policies. This is based upon a specific method imposing a rigorous structure of the processes. The assurance level will be reached when a structured system is built up, when all components of the system are mastered.

The first stage requires a structure regarding Information Security in order to evaluate every function of it. In order to gain assurance in the system, a formal structure, dissecting all the components of the system is needed.

The Information Security Level of a given organization will derive from the performance quality of each one of these activities. Taken together, the measured performance of each activity will allow an overall evaluation of whether the global Information Security Level has been satisfactorily attained.

By considering security as a process, and quality as an inherent feature and as a degree of excellence, thus the quality of Information Security is the degree to which a set of inherent characteristics fulfils requirements. In our case, it will have the look of the PDCA model including:

1. Management responsibility
2. Resource management
3. Product realization
4. Measurement analysis and improvement.

Last, but not least, organizational requirements have to be evaluated in order to assure that the Information Security System in place performs in an efficient (reasonable) way. This could be performed by measuring or assessing the security system maturity, which indicates the extent to which a specific process is defined, managed, measured, controlled and effective; this improves, according to [21], the predictability, the control and the process effectiveness.

5. A case study

A large manufacturing company with operations in more than twenty countries and significant IT centers in ten different locations became aware that it had very little consistency in its approach to risk assessment, security assessment and practical security measures, partly as a result of different infrastructures and application environments in different territories, and partly as a result of the historical ad hoc nature of the development and implementation of policies, procedures and internal controls. It used the opportunity provided by the introduction of the Sarbanes-Oxley Act to re-evaluate its security management from the top down and to implement and reinforce a structured approach to protecting its assets.

The first phase of the project involved a detailed review of the overall corporate risk assessment. By necessity this was driven by the need to evaluate the risks that the group encountered in respect of its financial reporting obligations, but the project was deliberately set a wider scope to incorporate elements such as operational, legal, environmental and reputational risk, and detailed questions relating to the utilisation and management of IT systems and data. The phase was led by a high-level team from corporate finance and compliance and obtained significant input from specialists in the legal and technical fields, with particular attention being paid to local requirements that were not necessarily visible from the corporate centre.

The second phase consisted of the definition of a series of control objectives designed to mitigate the risks previously identified. The objective here was to create a common structure that would be applicable across the whole group, without reference to the individual circumstances and application environments at each data centre.

The third phase involved the definition of specific control activities designed to implement the control objectives previously identified. Again, the aim was to provide as standard a template of controls as possible so that the activities performed in each data centre and by each infrastructure or application ownership group were as consistent as possible, but it was understood that complete consistency would be difficult to enforce and so some latitude was permitted to take account of local circumstances, as long as any deviations were documented, justified, and approved by the centre.

A critical reflection during this phase concerned the cost-effectiveness and the efficiency of the controls being designed. Management wanted to obtain an appropriate level of comfort and assurance over security without incurring excessive costs in the provision of new hardware and software, in training, or in employing new resources to perform the control activities in question. In addition, management wanted to ensure that the procedures implemented would be of appreciable added value to the organization and not tie up valuable resources in what would be seen as purely administrative, form-filling exercises. Accordingly, the control design process involved careful reflection on the nature and coverage of the control activities to ensure that sufficient comfort could be obtained from the effective operation of the smallest possible number of high-level, high quality controls, and preferably those that generated minimal overheads to implement and operate.

The next phase concerned the implementation of the controls, which involved the presentation of the controls matrices and supporting documentation to control owners, targeted training for those staff, and the acceptance of deadlines for the effective implementation of the new or formalized activities.

Some three months after the structured control matrices for security were implemented, management began to evaluate the operational effectiveness of the controls. As a first step, local management was asked to confirm their compliance with the new standards and indicate any areas of difficulty in implementing or operating the controls. Then corporate internal audit performed reviews for each site, looking for evidence of the operation of controls. A final phase saw the external financial auditors review the operation of controls for a sample of sites. The results of all three steps were amalgamated into a reporting package that was discussed and reviewed by senior IT management, corporate management, and the CIO's office.

As a result of these reviews and of the feedback obtained from control owners, a number of modifications were made to the overall structure of controls and to individual control activities, in order to clarify, simplify, or make them more effective and efficient. Senior management also set up a procedure for the annual review of the entire process, starting with the risk assessment and drilling down towards individual controls, in order to ensure that significant risks continued to be addressed and that resources were being focused in the correct directions, all the while complying with the corporation's stated objectives for maintaining an appropriate level of security.

6. Conclusion

The notion of survival brings to mind the long-term preservation of resources and, by analogy, sustainable development.

If we consider the question of sustainable development: what has changed today is man's ability to understand the gravity of the situation and to demonstrate its mechanisms, combined with the previously missing technical capacity to analyze and understand the elements of sustainable development and their interactions. Sustainable development is based on the preservation of resources of the space capsule that our planet is, and their value for future generations.

The objective is to preserve the resources of our enterprise, to make them multiply, to appreciate their value relative to their potential loss and to not sacrifice the criteria of economic efficiency to the hurdles of short-term profitability.

We should not economize on resources for risk management and the establishment of efficient and sustainable security solutions as these are critical steps when addressing problems with disastrous consequences.

This questioning of the enterprise's sustainable development leads us back to considerations concerning the notions of good governance.

7. References

[1] P. Bowen, J. Hash, and M. Wilson, *Information Security Handbook: A Guide for Managers (NIST Special Publications 800-100)*National Institute of Standards and Technology, 2006. [Online] Available at http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

[2] C. P. Grobler, "A Model to assess the Information Security Status of an organization with special reference to the policy Dimension", M Phil (IT) Thesis, Computer Science Department, University of Johannesburg, 164, 2003.

[3] IFAC, *Enterprise Governance: Getting the Balance Right* International Federations of Accountants, Professional Accountants in Business Committee (PAIB), 2004. [Online] Available at http://www.ifac.org/MediaCenter/files/EnterpriseGovernance.pdf

[4] ITGI, *Information Security Governance: Guidance for boards of Directors and Executive Management, 2nd Edition*IT Governance Institute
, 2006. [Online] Available at http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=24384

[5] *ISF-std. The standard of Good Practice for Information Security* Information Security Forum, 2007.

[6] W. R. C. Latin_America_and_the_Caribbean, "RIO DE JANEIRO COMMITMENT: REGIONAL PREPARATORY MINISTERIAL CONFERENCE OF LATIN AMERICA AND THE CARIBBEAN FOR THE SECOND PHASE OF THE WORLD SUMMIT ON THE INFORMATION SOCIETY " 2005. [Online] Available at http://www.itu.int/wsis/docs2/regional/declaration-rio.pdf

[7] T. Peltier, "Risk Analysis and Risk Management " *Information Systems Security* vol. 13 (4), pp. 44-56, 2004.

[8] *IEEE-Std. 1700, IEEE P 1700: Information System Security Assurance Architecture (ISSAA) Standard,* IEEE, USA 2008.

[9] AIRMIC, ALARM, and IRM, "A Risk Management Standard," The Institute of Risk Management, The National Forum for risk Management in the Public Sector, The Association of Insurance and Risk Managers, London, UK 2002. [Online] Available at http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf

[10] U. Beck, *La société du risque : Sur la voie d'une autre modernité*. Paris, France: Flammarion, 2008.

[11] F. Cohen, *IT security governance Guidebook with security program metrics*. Boston, USA: Auerbach Publications, 2006.

[12] B. v. Solms, "Information Security - The Third Wave," *Computers & Security,* vol. 19 (7), pp. 615-620, 2000.

[13] K.-L. Thomson and R. v. Solms, "Towards an Information Security Competence Maturity Model," *Computer Fraud & Security,* vol. 2006 (5), pp. 11-15, 2006.

[14] M. Johnson and J. Spivey, "ERM and the Security Profession," *Risk Management,* vol. 55 (1), pp. 30-35, 2008.

[15] *ISO-Std. ISO/IEC TR 13335-1, Information Technology - Guidelines for the management of IT Security - Concepts and models for IT Security,* International Organization for Standardization (ISO), Switzerland, 1996.

[16] *ISO-Std. ISO/IEC 27005:2008, Information technology - Security techniques - Information Security Risk Management,* International Organization for Standardization (ISO), Switzerland, 2008.

[17] *ISO/TC-Std. 31000:2008, Risk Management - Principles and guidelines on implementation (draft),* International Organization for Standardization (ISO), Switzerland, 2008.

[18] ENISA, "A Users' Guide: How to Raise Information Security Awareness," European Network and information Security Agency, Heraklion, Greece 2006. [Online] Available at http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_a_users_guide_how_to_raise_IS_awareness.pdf

[19] *ISO-Std. ISO/IEC 15408:2005, Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model,* International Organization for Standardization (ISO), Switzerland, 2006.

[20] S. Posthumus and R. v. Solms, "A framework for the governance of information security " *Computers & Security,* vol. 23 (1), pp. 638-646, 2004.

[21] *ISSEA. Systems Security Engineering Capability Maturity Model (SSE-CMM),* International Systems Security Engineering Association (ISSEA), 2003.