Developing strategic perspectives for enterprise risk management towards information assurance

Chatzipoulidis Aristeidis[1], Ioannis Mavridis[1], Theodoros Kargidis[2]
[1]Department of Applied Informatics, University of Macedonia, Thessaloniki, Greece
[2]Department of Marketing, Alexander Technological Educational Institute, Thessaloniki, Greece
chataris@uom.gr
mavridis@uom.gr
kargidis@mkt.teithe.gr

Abstract
Information is an important key business asset, which can exist in many forms, it involves various risks and it is essential that is suitably protected. Therefore, it requires the involvement of proper management ensuring that information assets are sufficiently secured and controlled. Truth is that the risk management discipline has received increasing attention in recent years due to increased regulations, ongoing changes and greater economic volatility that all affect the business environment. The purpose of a proper risk management action is to ensure transparency at all levels of the organization by taking the appropriate measures to reduce costs and manage financial, organizational and personal risk all at once, satisfying business objectives. However, due to misleading fallacies around its concept and the complexity that derive from governance, risk and compliance (GRC) activities, risk management falls short of assuring information assets. In this paper the results of our work on studying government, compliance and human factors in information security risk management are presented. The scope is to develop strategic perspectives around risk management implementation related to the concept of information security, helping minimize risks and cost. Sustaining security value over long term necessitates the realization of the information security lifecycle and the recognition of an imperative factor, the human involvement. Security spending remains a main concern despite the current economic crisis showing challenges that need to be confronted. Such challenges include maintaining a strong IT workforce, addressing growing foreign and domestic competition, developing critical infrastructure protection, balancing automated and manual controls and controlling intellectual property rights. The road ahead is the recognition of an enterprise risk management (ERM) strategy able to maintain security assurance and challenge ongoing changes that impact on the effectiveness of risk management. In addition, it is high time to consider a wider risk management approach, that of the societal risk management. For optimized results, the organization should foster a culture based on communication and feedback, recognizing training and security awareness a top priority. Creating a holistic picture of an enterprise as part of risk management and compliance efforts, it will provide a comprehensive platform for capturing and integrating multiple perspectives on processes, thus controlling information flow. Information assurance depends on the level of collaboration across internal and external parties and the correlation of disperse information. To avoid unpleasant circumstances, the risk management principle should engage into a dual approach of operability, that is maintaining performance and periodically re-evaluate itself to tackle with upcoming trends and risks.

Keywords: Information security, Risk management, Compliance, Human factor, Strategy

Introduction

Since the recognition that information assets play a critical role for each and every organization's long term survival, the information security concept has utterly changed. Companies have all gained experience in securing personal information resources in one way or another, either by deploying strict supervision controls or by complying with international security regulations and practices. However, all acknowledge the necessity to introduce more focus and more corporate parameters into the process of information security because standards compliance does not equal a sound risk management process. Regulatory security standards are intended to provide a generalized baseline for information protection but organizations usually fail to recognize their own security requirements. In reality, most do not directly map security requirements to any single standard or set of standards. Organizations tend to invest heavily in compliance programs that are prone to confuse security efforts with risk management. Even so, it is the very elements within an organization that do not overlap with a standard may present the most challenging risks (Rohmeyer, 2009). This paper aims to develop a dual, enterprise, risk management approach towards information security since protecting important

organizational assets, such as information, is more a matter of balance controls, timing risk countermeasures, and decision-making rather than the actual compliance with security regulations or the need for strict policies.

Information security can be described as the process through which an organization protects and secures its systems, media and facilities that process and maintain information vital to its operations (FFIEC, 2006). Protection of information assets is necessary to establish and maintain trust between the organization and its customers, sustain compliance with the law and protect the reputation of an institution. However, the majority of organizations often inaccurately perceive information security as the state or condition of controls at a point in time. In fact, security is an ongoing process that is prone to change posture while reacting to risks, technologies and business conditions. Therefore, it is becoming increasingly obvious that inappropriate security measures can have a negative effect on the overall business operation. Regardless of the solutions employed to reduce the risk of data security breaches, a balance in prevention strategies and risk mitigation efforts is likely to provide the best possible solution.

But while risk is a natural and indispensable part of business growth, unmanaged risk can quickly lead to chaos and expose critical data and resources to attack. To prevent exposure, change management procedures are considered proactive elements able to help companies ensure that policies and approvals are met before a change to the system occurs (Nagaraj, 2009). Sustaining security value involves the utilization of risk measures in accordance with the business objectives and security requirements. Understanding how the stages of security application lifecycle and business economic cycles affect the overall security approach is of critical consideration. The road ahead is the emergence of a dual enterprise risk management strategy able to attain security performance during turbulent times and change dynamically in accordance to metrics, trends and time. Additionally, the acknowledgement that technology itself can do everything but harm shows that human factor is considered the weakest part of a security system (Hinson, 2003). Cultivating an organizational culture based on continuous training and security awareness programs is key to sustain security value at a profitable growth.

Sustaining security value

It is surprising how many organizations continue to stimulate interest towards information security despite the current economic turndown. In the face of new trends firms deploy strict safeguards to serve one of their most profitable asset, the information records. However, what have been missing is that most defenses soon lose their potential to create enough security and a long lasting competitive advantage. The more they are diffused, the more they become standard-used by competitors. In fact, there are very few strategic assets available to a company that can provide long term differentiation. Information security is one of them, along with brands, innovation, a cost-efficient culture and the ability to adapt rapidly to change (Kapferer, 2004). Security practices may serve as effective means of starting the process of improving security, yet, in the long run, companies usually become vulnerable to theoretical guidelines. Paradoxically, it takes more than technology to build security.

A sole reliance on international security practices, such as ITIL, COBIT or ISO 27000 series, may result in inappropriate spending decisions and unforeseen complexity. In the past, the implementation cost for similar programs, controls and countermeasures to classify security information was deemed non-quantifiable, accompanied with other overhead expenses. However, the changing landscape of information security and the impending recession impacts on everything and information security spending in no exception. A forthcoming challenge for organizations is how to reduce information security costs while ensuring maintenance of sufficient controls against risk. Managing risk is all about taking it down to acceptable and manageable levels, being pragmatic and able to justify every security investment decision (SANS, 2002). But how much security is enough to sustain security value?

Interestingly, security does not appear in balance sheets and its intangible character propels the factor of the unknown. Security awareness, trust, image and reputation, all build over the years, are the best guarantee for future earnings but the essence is all about the value of information security an organization possess and delivers to employees and to the broader public. First, the value of information security lies in its capacity to generate cash flows and promote business activities. Second, security is considered a conditional asset, meaning in order to deliver results it needs to work in conjunction with other tools such as personnel training, compliance with security mandates and

audit testing. Security assessment starts with creating inconsistently applied security efforts and countermeasures throughout the enterprise and optimizes when security becomes culture-centric, attached to a viable economic business model (KPMG, 2008). Therefore, if a business cannot profit from security, it is doubtful that security has any value. It may have great potential, as measured by various associations evoked in consumers' minds for controlling risks but such potential needs a profitable economic equation to become justifiable. In real terms, information security must be a time and risk reducer. The perceived risk could be economic, functional, social, experimental or even unknown. The point for security to exist in information systems and provide a state of assurance is to acquire the power to maintain, control and change during time. Forecasting and trend-spotting should become more important in the quest for innovations that provide a reasonably competitive advantage. Selected compliance with security mandates can benefit an organization via revenue growth, protection against financial and reputation loss, efficient business continuity, proactive regulatory compliance and protection from loss of intellectual property. Alternatively, noncompliance penalties can be overwhelming and vary from loss of reputation, financial penalties and most important a possible breakdown in the integrity of the system (PriceWaterhouseCoopers, 2009).

The majority of concerns with respect to security issues can be addressed via the different stages in a security application life cycle (Corsaire, 2008). Specifically, during each stage of application lifecycle, security operates differently. In the development stage, security requirements needs to be identified and documented in order to provide a conceptual platform for evaluation and analysis. In the deployment stage, security testing is paramount since this ensures that systems can recover easily in the event of failure and can also assist in reforming the system administration. In the maintenance stage, all necessary security patches and updates should be regularly tracked and applied. Change is a necessary part during a security period so before adjusting to a new environment, feedback analysis is essential for avoiding possible security and business implications. Understanding the security application lifecycle is critical to set consistency and manage security operations during implementation. But security does not work alone. Similarly, business operations and the general economic situation affects the effectiveness and efficiency of an information security program. From business expansion until recession, the value of information varies and priority becomes information consistency at all costs in order to avoid unwanted situations such as a breach in confidentiality, availability and integrity of information systems. The National Institute of Standards and Technology (Kissel, 2009) recommends that business should focus on what their business actual needs are, protect and manage them, dispose of what is outdated and plan ahead by monitoring and responding to security and business incidents.

Information security spending

The ongoing economic downturn affects nearly all sectors of the economy and the information security industry is not left invulnerable. But against this trend, there is a clear growth in the need for information security services driven by increasing risks and compliance requirements. Information security is usually controlled by upper management who tends to establish sound risk management processes in order to optimize the efficiency of an information security infrastructure (Lacey, 2009). Reality is that every organization is looking to reduce costs and improve the effectiveness of information security spending programs in an attempt to maximize security investment and protect vital intellectual property while satisfying various stakeholders' interests. However, while such investments on security tend to decline, companies with insufficient IT security spending are prone to face a more risky scenario through which their overall security approach might suffer.

Zisser survey results (Zizzer, 2009) reveal that most people perform security and compliance measures internally while the majority of respondents want to leverage classification and free-trade data for strategic purposes but are currently unable to do so because of deficient visibility by upper management. Related research (Imperva, 2009) reflects that companies struggle to protect consumer data. In fact, 71% of companies surveyed refrain from making data security a top strategic initiative but the minority who deploys the GRC (governance, risk and compliance) discipline strategically achieves fewer data breaches. Key findings of another study (Gartner, 2009) reveal that organizations that have suffered a public data breach spend more on security in the development process but only 67% of surveyed firms have a specific IT security budget. Goldman Sachs predicts raising in global IT spending for 2010 (Goldman Sachs, 2009) while another survey (Yoran, 2009) reveals that the most influential driver of IT security spending is compliance, followed by threat reduction and brand

protection. In the IT security sphere, governance, risk and compliance management are leading security projects.

In an attempt to reduce costs while strengthening security, organizations should automate much of the security activities while keeping continuous human monitoring. This is because security controls are a mixture of software and hardware processes combined with human procedures so in order to make security programs less demanding will require the integration of business processes within the information security program. To avoid financial penalties for noncompliance, organizations need to cooperate with external groups, such as security auditors, who must enforce compliance controls and procedures regarded costly to deliver. Sun Microsystems, in an attempt to lower security costs, set in 2007 a course by proactively implementing IT controls and processes that would help protect financial applications and data from unauthorized changes. The program addressed both business and technical means via ensuring that financial data possess a high degree of integrity. Sun's strategy was to address the highest risk areas first and perform only the minimum and sufficient work needed to achieve compliance in these areas. Key results reveal that the program was a significant contribution since it succeed in reducing overall audit costs by 75 percent within two years (BTQ, 2008).

While the current economic situation has caused business to think twice about future investments, security spending is still of primary importance. Yet, even Harvard Business School will be forced to cut down operational expenditures that derive from security spending. The global IT security industry revenue for the year 2008 was recorded at $13.5 billion, up 18.6% from $11.3 billion during 2007 showing remarkable resilience against the current economic downturn, reviling that information security is a top priority (Gartner, 2009). Information assets will always require a shield of protection, because high quality information is considered the lifeblood of business superiority. Such information might be sensitive employee or customer information, confidential business research or plans, financial information or information falling under special information categories such as privacy and health. However, budget deficiency, increased regulation and the growing complexity that characterizes the information security environment (Fratto, 2009) are the ongoing menu for risk managers to deal with. Responsibly, security chiefs need to communicate the risk message clearly and smoothly to all partners, employees and broader public. Information security spending can be optimized when a proper balance is achieved between automated and human controls capable to standardize operations and also when human involvement is perceived as the most valuable form of security control.

The neglected human factor

Using technology to control information flow may not be the answer to information security problems. Security assurance is considered the highest state in an information security system and it can be succeed only when it is evoked in human minds. Moreover, information assurance inconsistently change at a fast pace. Technology alone cannot deliver sufficient security services in practice and this is where human involvement complicates things (Hinson, 2003). Despite the efforts to produce infallible software tools, attackers and risks still find the way to breach information systems. Taking into consideration the increasing costs that derive from security software updates, building an organizational culture centric to risk mitigation strategies may be the most cost effective approach to information security. Many authors have outlined the importance of human participation in information security but have also acknowledged human factor as the weakest part in a information computer technology (ICT) infrastructure (Sasse et al., 2001). Certainly, human behavior has no standards and the problem becomes even worse when people with different personalities or cultures need to work together under time pressures or financial constrains.

Further, risk perception is highly volatile among users and is affected not only by technological improvements but also by the behavioral regulation theory (Gonzalez and Sawicka, 2002). In fact, people can be either the weakest or the strongest link in the security chain. Achieving the latter is possible with executive involvement, the assistance of security professionals, cross-functional corporate input and scheduled independent reviews (Egan, 2005). High priority issues regard staff competency, encompass the capability of management, the changing staff behavior, the communication of security incidents, the education of senior managers and their responsibilities as role models, the changing perception towards security and the fraud prevention at all levels throughout the enterprise. No less significant is the employee training process as part of security

awareness programs that are developed to update and sustain a culture of precaution within an organization. Security and risk management processes are evolving disciplines so moving from static actions to dynamic decision-making paves the way for a mature approach towards information security. However, even security-conscious professionals may be perceived as suspicious and this may reduce users' willingness to conform to rigorous security requirements. (Sasse et al, 2001).

According to a recent ERM Survey (Institute of Internal Auditors, 2009) only 40 percent of the 240 organizations examined have implemented a formal risk management program or process. In addition, overall risk culture factors as well as internal environmental factors play the most significant role in the organization risk management process. Exploiting human vulnerabilities may be the key to answer why ICT security infrastructures fail to accept an otherwise infallible risk management program. Bringing IT, physical and human security together under a holistic and unified information security management system reflects the coordination of various elements able to consist a portfolio of well-selected risk countermeasures. Particularly, when referring to human factor, this involves a group of experts relating to behavioral, assessment, selection and training activities who work together with statisticians and operational analysts under a common goal, to satisfy ICT security objectives (Shareeful and Dong, 2008). It is this combination of professional skills that can help increase the potential of technology and provide a pragmatic level of security towards information risk. Benefits that derive from such an approach is the reduced cost in information security spending through process improvements, elevated performance against risk and smoother integration of man and machine.

The road ahead

Historically, the field of risk management has been dominated by theoretical discussions, practical misfits and indecipherable algorithms all of them adding to complexity and little in essence. Even recent high profile corporate failures, that is said to have caused the current economic turndown, have highlighted the failure to identify and appropriately manage risk at a strategic level. The road ahead is not clear but research and development in risk management leads to the recognition that risk procedures should alter regularly profile and become inherit parts of an overall business mission focused to satisfy organizational objectives, security requirements and stakeholders' vision repeatedly. In other words, an enterprise risk management practice (ERM) is considered the evolution of static risk management procedures taking into consideration the changing economic, security and social landscape (Soo Hoo, 2000; PriceWaterhouseCoopers, 2009).

In general, risks emerge because of limited knowledge, experience, information and uncertainty regarding the future or through changes in the relationships between parties involved in an undertaking. Activities focused on risk protection share a common objective, to recognize and prepare for a range of possible future outcomes using a portfolio of risk countermeasures. The "ideal" organization should build a comprehensive data inventory, design and implement sophisticated security controls to reflect the value and sensitivity of the assets protected, manage security risk through a selected combination of regulatory compliance activities and continually assess and monitor the operating environment, constantly aware of blind spots and unknown activities. In case, the obstacle is that the majority of firms refrain from a dynamic behavior towards risk and most lack in risk communication effectiveness. Thinking like an attacker (Accenture, 2009) and acting systematically in view of security improvements is likely the best solution to adapt. Successful risk management requires, above all else, a solid grasp of what is going on across the organization and the ability to successfully interpret it in common terms. Hence, there is a need to move away from complex and costly approaches of maintaining different data for different functions and aim for a single, sustainable, integrated data warehousing system that is capable of managing risks on the basis of a sound enterprise risk management concept. ERM is considered different from traditional risk management techniques due to its holistic view to risk and the overall portfolio of security tools. COSO defines ERM (COSO, 2004) as "a process, affected by an entity's board of directors, management and other personnel, applied in a strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity goals". Organizational objectives for pursuing an ERM approach is to satisfy various stakeholders' values, surpass static risk methodologies, increase transparency of operations and communicate decision making across the organization.

Key theme in the growing of an ERM approach is the nurturing of a risk management culture. This is the general approach of a firm dealing with risks under certain rules of behavior known as codes of conduct and corporate ethics. Usually, training and security awareness programs are means of promoting security consciousness within an organization. However, their effectiveness depends on strategic decisions and the risk position an organization reflects against liable threats. ERM is a process in which components influence one another. This inter-relationship between different organizational components affect the efficiency and effectiveness of a security risk program. For example, the structure of an internal environment may affect control activities or the ability to communicate risk may affect monitoring or decision-making and vice versa. Still, even solid ERM practices do not provide the basis for a perfect security environment, but such do not exist. Limitations are frequently considered the human judgment towards risks, mistakes and errors that can result from fatigue, distractions or lack of training and experience and less frequently technology itself. Additionally, any security investment or decision must be weighed against existing resources, aiming at a positive return on investment (ROI). One of the greatest challenges in constructing an effective ERM system is identifying and gathering not only relevant information from various departments within the organization but different data from outside the scope of mainstream operations. Achieving superior risk management propels the mobilization of an organization's entire risk community, ranging from partners to audit consultants and from senior managers to employees.

Governance, compliance and risk issues require an understanding of the opportunities as well as the vulnerabilities but this depends on the ability to adapt smoothly to change. However, putting it simply a change management process in action is not enough. In fact, if an organization engages in a change management process in order to "preserve secured" the point is far absent. Change management should integrate seamlessly into the overarching risk management program by decreasing approval times for critical changes, keeping the firm moving forward. Such is the point behind a dual approach to enterprise risk management. Sound examples of ERM effectiveness come from General Motors, Lewis and Wal-Mart, companies who use ERM initiatives to strengthen governance processes via the internal audit function (Walker et al., 2003). Organizations have the opportunity to gain a competitive advantage by using compliance efforts to build balance controls that are sustainable and add long term value to the organizational structure. The backbone of any compliance strategy (Backman, 2007) is sound technology that can deliver the necessary checks to clarify grey areas that exist around corruption and corporate culture. Moreover, transparency of operations has also highlight the importance of the societal risk management notion within the core of an ERM process. Green compliance is gaining increasing merit because progress leads to a more complex society. Addressing society's interests on a coordinated basis should become central to the responsibilities of an ERM practice. Defining quality risk management processes that entails to minimize risk on the concept of moral commitment is considered strategic thinking strengthen for success.

Conclusions

The majority of organizations struggle to conform with corporate laws and regulations and this effort has caused the employment of resources and budgets to a non-profit activity, which is regarded as more as a running cost rather than an investment. Such efforts brought up the need to establish monitoring controls in order to standardize much of the processes but the overhead costs incurring from staff and management turnover tend to diminish the profile of a security system. Put it simply, automated controls may help in standardizing operational procedures but are not the answer to reduce complexity of an information security initiative. Achieving sufficient security levels calls for a deeper understanding of the processes, organizational objectives, enabling technology and the inconsistent risk of occurrence. Thus, it is recommended for organizations who are interested in achieving security assurance to select and adapt security practices, such as the ISO 27000 series, in accordance with the unique culture and risk appetite. Such related security acts and policies may seem expensive to acquire and time-consuming to adapt hence a methodical selection of security regulations in relation with the organizational objectives is supposed to optimize security spending and yield a positive return on investment.

Moreover, having experienced people who understand the fundamentals and know-how to think critically, strategically and creatively is considered key element in maintaining security performance while shrinking business budgets do not allow additional security investments. In reality, the risk management concept requires serious changes in order to cope with compliance, audit and

governance evolving issues. Usually, the failure to manage and monitor risks derives from the loss in communicating risks in common terms and from the inappropriate selection of risk metrics. A dual, enterprise, risk management approach can help business entities assess and enhance internal control systems by constructing an ICT management framework capable to incorporate policy, rule and regulation issues into a single approach allowing smoother control of the information flow in due diligence. Among the most critical challenges for risk management is how much risk the entity is prepared to accept as it strives to create and sustain security value. The latter is optimized when proper balance between automated and human controls and between growth and return goals is achieved. In a globalized, interconnected and competitive world, the need to compete successfully requires the convergence of IT, physical and human involvement in an integrated approach towards risk.

To conclude, managing risks involves a diverse range of activities from risk assessment to monitoring and from reviewing results to forecasting trends. During this process, risk communication is an interactive process of information and opinion exchange about risk awareness among involved parties. Embedding a dual, enterprise, risk management approach into the core of an ICT infrastructure will provide differentiation on the basis of proactive risk anticipation and social responsibility.

References

Accenture, (2009), "Managing Risk for High Performance in Extraordinary Times", Report on Global Risk Management Study, [Online], http://www.accenture.com/Global/Consulting/Finance_and_Performance_Mgmt/Risk_Management/Research_and_Insights/ManagingStudy.htm

Backman, A., (2007), "If Compliance Is So Critical, Why Are We Still Failing Audits?", Information Systems Journal, Vol. 5, [Online], http://www.isaca.org/AMTemplate.cfm?Section=20075&Template=/ContentManagement/ContentDisplay.cfm&ContentID=44793

BTQ, (2008), "Reducing the Cost of Compliance", [Online], http://www.btquarterly.com/?mc=reducing_compliance&page=grc-viewarticle

CORSAIRE, (2008), "Application Security and the Secure Development Lifecycle: Changing the status quo", [Online], www.auscert.org.au/download.html?f=220

COSO, (2004), "Enterprise Risk Management - Integrated Framework, September, [Online], http://www.circulo-icau.cl/uploads/documentos/descarga_0/coso008.pdf

Egan, M., (2005), "Information Security and the Human Factor", [Online], http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=25110

FFIEC, (2006), "Information Security Booklet", July, [Online], http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf

Fratto, M., (2009), "Strategic Security: A Struggle For Balance", [Online], http://i.cmpnet.com/custom/strategicsecurity/assets/InformationWeek_Analytics_2009_Strategic_Security_Survey.pdf

Gartner (2009), "Global IT Security Spending Rising Unabated Amidst Recession", [Online], http://ow.ly/164LL4

Goldman Sachs, (2009), "Goldman Sachs Raises 2010 Outlook for IT Spending", [Online], http://abcnews.go.com/Technology/wireStory?id=8633457

Gonzalez, J., J., Sawicka, A., (2002), "A Framework for Human Factors in Information Security", [Online], http://ikt.hia.no/josejg/Papers/A%20Framework%20for%20Human%20Factors%20in%20Information%20Security.pdf

Hinson, G., (2003), "Human factors in information security", Whitepaper, [Online], http://www.infosecwriters.com/text_resources/pdf/human_factors.pdf

Imperva (2009), "PCI DSS Security Standards Council Compliance Survey Results", [Online], https://www.imperva.com/ld/ponemon.asp

Institute of Internal Auditors (2009), "2008 ERM Benchmarking Survey, Executive Summary", [Online], www.theiia.org/download.cfm?file=68594

Kapferer J-N., (2004), "The new strategic brand management: Creating and Sustaining Brand Equity Long Term", 3rd edition, Kogan page, pp. 198-246.

Kissel, R., (2009), “Small Business Information Security: The Fundamentals”, [Online], http://csrc.nist.gov/publications/drafts/ir-7621/draft-nistir-7621.pdf
KPMG, (2008), “Governance, Risk and Compliance. Driving value through control monitoring”, [Online], http://www.kpmg.ca/en/services/advisory/documents/GovernanceRiskCompliance.pdf
Lacey, D., (2009), “The impact of the recession on information security spending”, [Online], http://www.computerweekly.com/blogs/david_lacey/2009/06/the_impact_of_the_recession_on.html
Nagaraj, P., (2009), “Enabling effective change management with an integrated change control mechanism”, Whitepaper, [Online], http://ca.com/files/WhitePapers/33822-eff-chg-mgmt-mp_204230.pdf
PriceWaterhouseCoopers, (2009), “Enhancing performance through control optimization”, [Online], http://www.pwc.com/en_CA/ca/controls/business-process-controls/publications/enhancing-performance-2009-06-10-en.pdf
Rohmeyer, P., (2009), “Standards compliance does not equal sound information security risk management”, [Online], http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1373558,00.html
SANS Institute, (2002), “Building and Implementing an Information Security Policy”, [Online], http://www.sans.org/reading_room/whitepapers/policyissues/building_and_implementing_an_information_security_policy_509
Sasse, M.A., Brostoff, S., Weirich, D., (2001), “Transforming the 'weakest link': A human/computer interaction approach to usable and effective security”, BT Technology Journal, Vol. 19, No. 3, pp. 122-131.
Shareeful, I., Dong, W., (2008), “Human factors in software security risk management”, International conference on software engineering, pp 13-16, [Online], http://portal.acm.org/citation.cfm?id=1373312&dl=GUIDE&coll=GUIDE&CFID=65354987&CFTOKEN=16998977
Soo Hoo, K., J., (2000), “How Much Is Enough? A Risk-Management Approach to Computer Security”, Working paper, [Online], http://iis-db.stanford.edu/pubs/11900/soohoo.pdf
Yoran, D., (2009), “Information security spending survey 2009 results, [Online], http://metrosite.files.wordpress.com/2008/06/information_security_spending_survey_2009.pdf
Walker, L. P., William, G. S., Barton L. T., (2003), “ERM in practice: examples of auditing's role in enterprise risk management efforts at five leading companies shed light on how this new paradigm is impacting audit practitioners” [Online], http://findarticles.com/p/articles/mi_m4153/is_4_60/ai_106863370/?tag=content;col1
Zisser Customs Law Group (2009), “Winter 2009 ICPA Survey Results”, [Online], http://www.zissergroup.com/images/uploads/Zisser%20Survey%20Results%20Detail.pdf