EVOLVING CHALLENGES IN INFORMATION SECURITY COMPLIANCE

Chatzipoulidis Aristeidis, Department of Applied Informatics, University of Macedonia, Egnatia 156, Thessaloniki, Greece, chataris@uom.gr

Mavridis Ioannis, Department of Applied Informatics, University of Macedonia, Egnatia 156, Thessaloniki, Greece, mavridis@uom.gr

Abstract
With the proliferation of computer-driven organizations and internet-based business information systems, the need for security has increased significantly. In addition, information security compliance is becoming a controversial issue among IT professionals. This paper aims to address the concerns arising from compatibility of security standards, compliance cost, certification approval and human involvement that affect compliance management. A unified approach to information security compliance is suggested for organizations seeking to build strong relationships across business and IT departments, improving in that way a company's security value.

Keywords: *Certification, compliance, IT security, standardization.*

1 INTRODUCTION

Due to the increased reliance on information technology (IT) and digital content, the value of information assets has increased significantly. Organizations depend mainly on IT in order to provide a standard operating environment for conducting business activities. As a result, controlling risks to personal information via enhanced proper security controls has become a critical subject. Moreover, the failure to defend personal information can certainly result in high financial and public cost and may also cause disruption of business activities (Simon, 2008). To comply with security practices, enterprises must not only develop comprehensive information security programs but also manage effectively security procedures and controls. In case organizations fail to approach information security compliance in a systematic and integrated way, this results in incomplete, redundant or expensive security controls and procedures.

Although the use of security standards targets the establishment of specific countermeasures and safeguard policies, it is rarely specified which type of enterprise is compatible with particular security practices (e.g. ISO 17799 or NIST 800 series). As a result, the need for compliance has caused many misfits within the organizational society and the most profound reasons are the ambiguous compatibility of security standards, the increased cost towards compliance and the requirement for the certification of security standards (Heiko & Sabelfeld, 2003; Waxer, 2006).

In order to provide a common understanding of terms, a compatible security practice can be described as the process through which the enterprise determines which laws, regulations and guidelines are applicable to the organizational structure of the institution (Compliance Management System, 1996). In fact, the growing number of laws and regulations illustrates how complicated can become to match the requirements of security guidelines and standards within the organizational structure and business operations. A direct outcome from the increasing number of information security operations and

practices is the cost of compliance which can be described as the total amount of time and money spent in conforming to security requirements such as security laws, regulations and practices (McGilliduddy, 2006). A key element in compliance cost is information security training. Employees, staff, partners and managers need to be trained on their responsibilities concerning safe and secure information processing practices. Being able to justify the level of expertise in business staff and to acknowledge secure operation practices, security and business professionals tend to require the certification of compliance as a token of operational and compliance excellence. Given the changing nature of technology and the evolving risks, certification of compliance is described as a process of vigilance through which information security practices are monitored, tested and reviewed in constant mode (Pink Elephant, 2008). In addition, certification of compliance can take the structure of an assessment process which aims to certify that business departments are highly complying with all applicable security laws and regulations.

The information security operations are ongoing processes and this is due to constant changes in the regulatory landscape, including the creation of new requirements or the extension of old ones. As a result, this necessitates the management of security operations and procedures, known as compliance management (Leading Edge Forum, 2007). Defining compliance management, this is the procedure through which the enterprise manages the entire compliance process from scratch. A complete compliance program consists of policies, procedures and risk assessment tools which guide employees adherence to laws and regulations. This procedure addresses all phases of securing systems and networks including assessment, control and response feedback for unremitting performance (Adler, 2006).

The main purpose of this paper is to explore the challenges that compliance management face on the grounds of ambivalent compatibility, compliance cost and certification procedures in order to improve the efficiency and effectiveness of managed IT service standards. Additionally, a unified approach is recommended on the principles of driving technology innovation and reducing organizational costs; thus boosting performance and usefulness of security practices to a higher level of expertise.

2 CUSTOMIZING COMPATIBILITY AND CERTIFICATION

Once the scope of security compliance program is identified, the next step in a compliance approval procedure is the selection of the appropriate security method to ensure that the security standards are fully implemented in the context of the security compliance program of the organization (Jose, 2005). Normally, an enterprise applies audit and enforcement techniques to make sure that the security standards are being followed. As a result, the cost in time and money during security procedures should be justified as an internal business activity. However, the self-assessment of security practices has failed to offer adequate protection against information disruption. In fact, between February 2005 and July 2006, there were 237 reported security breaches involving the compromise of more than 89 million records containing personal information (Adler, 2006). These numbers reveal that either there were not adequate security controls and procedures in place to establish security compliance or the compatibility of security practices can never match the requirements of real industry operations. In fact, the level of compatibility depends on whether the organization structure can fit and adapt to a security policy framework (Pink Elephant, 2008; Johnson & Goetz, 2007).

Most recently, in search for increased compatibility, organizations pursue a certification of compliance and this often takes the form of licensed use documentation from a third party security consultant, such as HISP (Holistic Information Security Practitioner) or PinkVERIFY. HISP promotes a holistic approach to information security management by providing through a security system program certification for security practices such as the ISO 17799 (ISO 27002), ISO 27001, ISO 20000, COBIT, COSO and NIST guidelines. ISO 17799, which was renumbered in July 2007 and is now

known as ISO 27002, represents a security technique and code of practice for information security management. It provides information security professionals with specialized recommendations for risk assessment, physical and information security policy, governance, development, compliance and access control (International Organization for Standardization, 2009a). ISO 27001 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System (ISMS) within the context of the organization's overall business risks. It also specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts (International Organization for Standardization, 2009b). ISO 20000 serves as a widely recognized basis for evaluating IT Service management processes, providing measurable criteria that can be audited and defines requirements of service providers helping to determine whether the organization complies with acceptable service management standards (Kumbakara, 2008). COBIT stands for "Control Objectives for Information and related Technology" and it is an IT governance security framework that lists 34 high-level IT processes and audit guidelines to assess IT processes (Enterprise Strategy Group, 2008). COBIT recommendations include issues related to ensuring effectiveness and value of IT as well as information security and process governance. COSO (Committee of Sponsoring Organizations of the Treadway Commission) is an integrated security framework to help businesses and other entities assess and enhance their internal control systems (PwC, 2004). The NIST 800 Series (National Institute of Standards and Technology) is a set of documents that describe United States federal government computer security policies, procedures and guidelines. The 800series publications cover all NIST recommended procedures and criteria for assessing and documenting threats and vulnerabilities aiming to minimize the risk of undesirable events (NIST, 2008).

Similarly, PinkVERIFY is a worldwide independent assessment program that supports the workflow requirements of specific IT service management processes through a licensed logo and certifies Information Technology Infrastructure Library (ITIL) compatibility with operational security processes. ITIL provides a framework of best practices for managing IT operations. ITIL also recognises that there is no "one size fits all" solution to the implementation of processes for the management of IT operations (Kumbakara, 2008). Taking this approach one step further, the customisation of security practices can be the solution for the organizations who try hard to match business activities with selected security practices.

Efficient management and delivery of IT systems and services requires a mature approach regarding the implementation of an acknowledged security practice framework for managing IT services. Too often, organizations experience difficulty in delivering security practices into the organizational structure causing unexpected complexity and cost. The starting point with security practices, laws and guidelines selection should always be to first look at the way the IT processes function and interact (Mohamed, 2007). Of course, human involvement complicates security procedures since human behaviour is different in conception and utilisation from computer system behaviour. Although numerous published articles, journals, and books are filled with an abundance of information security guidance, few security guidelines are technically complex. Actually, the success of a security compliance program depends on whether the staff can adapt to a well defined security framework (Pink Elephant, 2008). Gasser (1988) wrote, "The problem is people, not computers" which means that information security professionals need to realize that they are a factor inside the equation that creates poor security compliance (Smith, 2009).

Given the abundance of security guidelines and standards, IT departments find themselves surrounded by a plethora of rules being initiated from different authorities, each of which may have a legitimate responsibility on certain business activities. Consequently, the real issue begins when other organizations establish rules for enterprise operations (Leading Edge Forum, 2007). Each organization is different in structure and security requirements; therefore information security compliance depends on whether customized policies and procedures can adapt to current or future security regulation and business environment. The security compliance process should be able to review technical, psychical

and administrative security practices and explicitly define how security policies and procedures are to be implemented and integrated with the current security and business activities and also how well business departments' work together to ensure that information security practises are harmonized and consistent (Pink Elephant, 2008). The organization information security program must ensure that all system users understand and follow information security practices and to manage that, a risk analysis assessment procedure should take place to gather, analyse and identify risks and the selection criteria prior to installing security practices.

3 TO BE OR NOT TO BE COMPLIANT?

Complying with ongoing government and industry regulations is a major concern for IT professionals and business managers. Whether it is ITIL, a compliance initiative or a specific industry regulation like HIPAA, these frameworks and guidelines provide a critical basis to secure vulnerable assets and information. However, security practices and standards can overwhelm organizations and introduce substantial unexpected costs and cause unforeseen consequences.

Time Warner, a media and communication company, has invested an enormous 350,000 man hours in identifying, evaluating and testing its financial and IT controls (Leading Edge Forum, 2007). According to a Forrester research, businesses across North American and Europe will spend more than 7.91 percent of their IT budgets on security in 2009, compared with 7.75 percent in 2006 (Waxer, 2006). Another study from Enterprise Management Associates (2006) illustrates just how severe shareholder impact can be when compliance fails to fulfil security standards. Stock prices fall like feathers in the wind but the worst scenario is that they never recover. Nevertheless, not everybody accepts the penalty of non compliance. Ponemon Institute LLC found that the cost of dealing with a data breach rising in 2008 by 30% to $4.8 million. Many companies refrain from securing their data until after they suffer a breach (Complinet, 2009).

According to a Deloitte global security survey (2007), information security compliance has risen in importance and is considered a critical area within business activities. Respondents listed their top 3 initiatives as "access and identity management", "security regulatory compliance" and "security training and awareness". When asked about their perceptions regarding the root causes of failures on information systems in their organization, respondents chose human error (79%), technology (73%), third-parties (46%), and operations (41%), respectively. Moreover, according to a recent survey by Complinet (2009), the cost of corporate compliance is expected to increase in 2009 and the reason behind the impending increase in compliance costs lies on the expectation of a tougher regulatory environment and the accompanying costs that will be necessary to deal with the ongoing changes. The same survey also reveals that compliance professionals anticipate increase in regulation, compliance costs and communication with regulators.

Compliance in information security requires a team effort that reaches from the highest levels of hierarchy (usually the CEO or Board) to the lowest level (employees) of workforce who are using the end results of the compliant components. The decision to adjust to a security framework depends heavily on the organizational management and transparency of operations. In order to reduce compliance costs while strengthening security, organizations should automate much of the security activity while keeping continuous human monitoring (Liberti, 2008). This is because compliance controls are a mixture of software programmed processes and human procedures so in order to make the compliance program less costly in time and money requires the integration of business processes within the information security compliance control. To avoid financial penalties for non compliance, organizations need to cooperate with external groups, such as security auditors, who must enforce compliance controls and procedures regarded costly to deliver.

4 TOWARDS A UNIFIED APPROACH

Compliance directives originate from government, trade associations, industry self-regulation and standards bodies. These rule makers attempt to supply an endless amount of laws, setting security standards around the globe. In reality, a single approach to security can not take place due to market diversification, yet the challenge is far greater. The speed of change is phenomenal, the risks affect all organizations without exception and there is no doubt that a comprehensive approach to information security compliance is needed. A growing trend within the business and IT professionals is the recognition that to effectively manage the IT environment, there needs to be a move away from a sole security approach towards an integrated framework of best security practices and procedures in order to maintain, process and control information security applications (Pink Elephant, 2008). Institutions looking to comply with regulations, secure their information assets and lower business risks should embrace a unified approach to information security compliance as an efficient and cohesive method to achieve and support information security protection. As a result, organizations have the opportunity to comply with multiple security practices and guidelines at one time.

Enterprise Strategy Group (2008) examined how the profile of an organization is affected when it uses multiple IT security frameworks from an organization who implements just one security framework or none at all. Findings revealed that organizations with multiple frameworks are subject to much more extensive regulatory and compliance pressures but most important, they tend to develop operational environments that foster cooperation and collaboration across business, IT and security. Organizations making current investments in ITIL, ISO and COBIT are often subject to significantly greater levels of external compliance pressure from those who choose to focus on a single set of security practices. Nevertheless, by its very nature, security practices and standards adherence is an unachievable goal and at the same time a continuous organizational commitment and procedure.

Organizations often find it difficult to achieve a strategic security approach that supports business goals such as driving innovation and reducing security costs to address compliance measures and protect valuable assets against internal and external threats (IBM, 2008). A team of highly trained professionals needs to be build in order to manage risks and coordinate security operations in a way that enforces compliance and optimizes business results. Security countermeasures and safeguards are considered optimal when analyzing risk in the context of the business goals and the outcome of risk analysis has a positive return on investment (ROI) (Kumbakara, 2008). In order to fulfil compliance goals, a unified approach to information security compliance needs to become the guiding influence for ensuring that all the different security domains work together in a holistic and synergistic manner, in configuration with the business objectives (Zuccato, 2006). Planning security management from a holistic perspective including business, IT and human involvement will enable organizations to successfully secure those business processes in a manner that provides the necessary evidence to demonstrate compliance (IBM, 2008). Institutions should also perform risk analysis and management techniques to validate that the security practices selection and implementation continues to be reasonable, effective and suitable to the organizational structure of each and every business entity. The results from risk analysis procedures usually take the form of a report which explicitly identifies threats, vulnerabilities as well as the selection criteria for the security countermeasures. Nothing is perfect, especially in security, thus the compliance process should be regularly monitored, tested, reviewed and modified against emerging risks and evolving threats.

The certification approval is a fundamental part of the unified process and has the role to confirm knowledge in information security systems and assurance. Information assurance is meant to be a secure development process which ensures that product security standards are state-of-the-art and applied consistently throughout the company. In this regard, the National Standards Registry Board (NSRB, 2009) clarifies on the principles of information security and assurance that in order to set long term protection needs, an organization should ensure through a strategic planning process a feasible

and realistic model to implement and enforce a logical and consistent information assurance infrastructure.

Nevertheless, a unified approach to information security compliance will not offer the expected results to business entities if security risks and the potential impact on IT are not communicated to executive peers and IT users in common terms (Burke, 2007). Education and training are key elements in a unified compliance process since people are the most important variables that need to be controlled and managed. In fact, technical security controls can be measured in a scale of technical evaluation but human behaviour towards security is difficult to predict and assess since it can not be planned, therefore, security awareness programs are considered essentials in a unified security compliance process.

5 CONCLUSIONS

The increased challenges towards information security compliance have caused serious incentives to implement comprehensive information security practices. A credible method of securing information assets is the successful use of multiple frameworks which indeed require business, IT and human cooperation. This is because security applies in all organization areas and affects operational procedures from different viewpoints. By adopting a unified approach to information security compliance, business institutions are expected to successfully manage the growing number of ongoing security risks because it is believed to create synergetic and stronger compliance efforts along with more consistent measurement and audit reporting.

Compatibility issues regarding security practices within the structure of the organization affect the operability of compliance controls and this depends on whether the organization has analysed and identified clear goals towards security requirements. The discovery process towards information security requirements includes risk analysis methodologies and assessment of system policies, network applications and of course constant evaluation towards human involvement. In addition, security practices compatibility is a non-stop effort of monitoring, reviewing and modifying security controls in order to optimise information security infrastructure, management and effectiveness of existing security policies and procedures. As a result, the certification approval will certify that the management and performance of selected security practices is professionally followed and maintained throughout the entire business operations. This is the logical aftermath of well defined metrics and tactics to secure information processing practices. Security practices accreditation should carry stringent tests for client data and employee security to defend proactively against fraud. Disrupting regular security procedures carries potentially serious civil and criminal penalties for non compliance.

In conclusion, while the compliance with laws and regulations can be costly in time and money, the price of non compliance is far worse and includes financial fines and public loss. Embedding information security into the organization pre-requires the rise of security understanding within the organization and the management of the most valuable information and business asset, the people. Building a secure organizational culture entails a sustained effort to collaborate organization departments and human activities towards business performance and security reliability.

References

Adler, M. P., (2006), “A Unified Approach to Information Security Compliance” EDUCAUSE Review, Vol. 41, No. 5, September/October 2006, pp. 46–61

Burke, J., (2007), "Nemertes Research", Network World [Online], Retrieved 26th May 2009 from <http://www.networkworld.com/research/2007/090707-compliance-cost-rising.html?page=3>
Compliance Management System (1996), Comptroller's Handbook, August 1996, [Online], Retrieved 20th March 2009 from <www.occ.treas.gov/handbook/cms.pdf>

Complinet, (2009) "Annual Cost of Compliance Survey 2009: More regulation with less resource means greater risk" (press release), [Online], Retrieved 20th March 2009 from <http://www.complinet.com/connected/news-and-events/press-releases/complinets-annual-cost-of-compliance-survey-2009.html>

Delloite Global Security Survey, (2007) [Online], Retrieved 21st March 2009 from <http://www.deloitte.com/dtt/research/0,1002,sid=1013&cid=170582,00.html>

Enterprise Strategy Group (2008) "ISO, ITIL and COBIT triple play fosters optimal security management execution" [Online], Retrieved 4th April 2009 from <http://www.scmagazineus.com/ISO-ITIL-and-COBIT-triple-play-fosters-optimal-security-management-execution/article/108620/>

Gasser, M., (1988), "Building a secure computer system", [Online], Retrieved 4th April 2009 from <http://nucia.ist.unomaha.edu/dspace/documents/gasserbook.pdf>

Heiko, M., A. Sabelfeld, (2003)," A unifying approach to the security of distributed and multi-threaded programs", Journal of Computer Security, Vol. 11.

IBM, (2008), "Take a holistic approach to business-driven security", Whitepaper March 2008, [Online], Retrieved 5th April 2009 from <ftp://ftp.software.ibm.com/software/tivoli/whitepapers/GMW14008-USEN-00.pdf\>

International Organization for Standardization (2009a), "ISO/IEC 17799:2005 Information technology - Security techniques - Code of practice for information security management" [Online], Retrieved 20th April 2009 from <http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm>

International Organization for Standardization, (2009b), ISO/IEC 27001:2005, [Online], Retrieved 6th April 2009 http://www.iso.org/iso/catalogue_detail?csnumber=42103

National Institute of Standards and Technology, (2008), "Technical Guide to Information Security Testing and Assessment", September 2008, Retrieved 4th April 2009 from <http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf>

Johnson, M. E., Goetz, E., (2007), "Embedding Information Security into the Organization", IEEE Computer Society, [Online], Retrieved 2nd April from http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=&arnumber=4218547&isnumber=4218538

José, A., (2005), "Security Metrics and Measurements for IT", The European Journal for the Informatics Professional, Vol. VI, No. 4, August 2005.

Kumbakara, N., (2008), "Managed IT services: the role of IT standards", Emerald Journal of Information Management & Computer Security, Vol. 16, No 4, pp.336-359

Leading Edge Forum (2007), Digital Trust, Compliance Management, Volume 4, [Online], Available: www.csc.com/aboutus/leadingedgeforum/knowledgelibrary/uploads/LEF_2007DigitalTrustVol4.pdf

Liberti, L., (2008), "CA Advisor Survey Results: Reduce Compliance Costs While Strengthening Security", published: 15 Aug 2008 [Online], Retrieved 4th April from <http://www.ca.com/us/eitm/collateral.aspx?cid=181392>

McGillicuddy, S., (2006), "Rising cost of data breaches fuels security spending", [Online], Retrieved 2nd April from <http://searchciomidmarket.techtarget.com/news/article/0,289142,sid183_gci1230148,00.html>

Mohamed, A., (2007), Information security: "The route to compliance" [Online], Retrieved 2nd April from <http://www.computerweekly.com/Articles/2007/04/24/223385/information-security-the-route-to-compliance.htm>

Paris, R., (2005), "Human Security Paradigm Shift or Hot Air?" The MIT Press Journals, [Online] Retrieved 21st March from <http://mitpress.mit.edu/journals/pdf/isec_26_02_87_0.pdf>

Pink Elephant (2008), "IT service management tools: compatibility considerations", [Online], Retrieved 4th April from <https://www.pinkelephant.com/NR/rdonlyres/3C232863-4423-430E-B5C6-8358A2D217B9/4340/PinkVERIFYServiceWhitepaperV333.pdf>

PriceWaterhouseCoopers, (2004), Enterprise Risk Management — Integrated Framework Executive Summary, September, [Online], Retrieved 2nd April from <http://www.coso.org/Publications/ERM/COSO_ERM_ExecutiveSummary.pdf>

Simon, E., (2008), "Introduction to the legal regulation of information society (in Robert Pinter coursebook "Information Society"), pp. 115-129.

Smith, J., (2009), "Critical Success Factor Survivability for Engaged Information Security Professionals, Auerbach Publications, [Online], Retrieved 6th April from <http://www.infosectoday.com/Articles/Critical_Success_Factors_Information_Security_Professionals.htm>

The National Standards Registry Board (NSRB), (2009), Principles of Information Assurance [Online], Retrieved 2nd April from <http://www.nsrb.us/PrinciplesofInformationAssurance.html>

Waxer, C., (2006), "The Hidden Cost of IT Security" [Online], Retrieved 21st April from <http://www.networksecurityjournal.com/features/hidden-cost-of-IT-security-041607/>

Zuccato, A., (2006), "Holistic security management framework applied in electronic commerce", computers & security 2007, pp. 256 – 265.