Global Information Assurance Certification Paper

Practical Approaches to Organizational Information Security Management

GIAC (G7799) Gold Certification

Author: Raees Khan, r.k@sent.com
Advisor: Rick Wanner

Accepted: August 10th 2010

Abstract

Over the past decade, information security has been one of the most sensitive areas of concern discussed at the senior management level for a majority of the world's leading organizations across all industries. In today's globally interconnected economy, with increasing reliance on technology to achieve competitive advantage amongst other objectives, information security is and has been by far one the most critical yet very complex and challenging requirement for conducting successful business on a global scale. Today's modern and technology-dependent organizations cannot afford to confine themselves with just the 'technical' aspects of information security, therefore in order for them to achieve their strategic business objectives, they need to foster a culture of analyzing, evaluating and treating information as a 'business issue' as opposed to 'technical issue' alone. This paper discusses a variety of highly insightful, practical and implementable approaches gained over a decade of international experience across the Asia-Pacific region, to assist organizations in an effort to effectively and efficiently manage information security in today's dynamic and ever-changing business and technology environments.

1. Introduction

All around the world, it has become a well-known fact, that a majority of the world's leading global organizations, across all industries, are constantly challenged in successfully achieving their strategic and tactical business and technology objectives in an effort to provide true-value to their stakeholders (COBIT, 2005). These leading global organizations increasingly rely on a variety of information assets, such as skilled personnel, complex business processes and the latest technology, to perform various functions across all divisions. These factors, when correctly provisioned, ultimately contribute towards successfully achieving the organizational objectives. However, one of the most compelling challenges encountered by these leading global organizations is the lack of clear and concise enterprise-wide view of organizational information security across the board (ISO/IEC 17799:2000/27002:2005).

2. Practical Approaches for Organizational Information Security Management

In the context of business and technology management, the word management generally refers to the ability to coordinate and conduct organizational activities in alignment with the policies and procedures set by the executive, to facilitate the organization's success strategy (COBIT, 2005). However, in the context of information security management, the word management usually refers to the necessary requirements and/or obligations to effectively initiate, plan, execute, monitor and control information security activities across the organization, in an effort to successfully achieve organizational security objectives; and to protect the organization from all potential threats – hence making it an indispensable process (COBIT, 2005). Below is a list of practical and implementable approaches, including a variety of globally recognized international standards and frameworks, which assist organizations to effectively and efficiently manage information security in today's increasingly complex and ever-changing environment.

Raees Khan, r.k@sent.com

2.1. Develop, communicate, roll-out and publish a comprehensive suite of approved organizational information security policies

The formulation, communication and publication of easily accessible information security policies, is by far one of the most critical controls an organization should consider implementing as per the ISO 17799/27002 Code of Practice for Information Security Management Standard. To facilitate effectiveness of information security policy, it is recommended that policies be written in a simple, standardized and a structured format; should be assigned clear business ownership; and lastly, should be a reviewed and updated on a regular basis with appropriate version control. An appropriate policy review and approval process should developed to perform this activity, as it demonstrates that the organization is committed to protecting critical business processes and assets, and has also obtained ongoing executive support for the maintenance of information security policies.

An organization's information security policy should not simply convey a plan of action, for example its purpose, goals, applicability, and activities; but should also document who is ultimately responsible for carrying out the security agenda across the enterprise. All personnel within the organization should be provided appropriate training on information security policy and the organization's security expectations, aligned to their functional roles. As an example, the corporate internet usage policy should be communicated, read, understood and acknowledged by all personnel within the organization, while a role specific policy such as the enterprise software management policy, should be scoped to include relevant personnel, for example the IT Systems department. It is also imperative for organizations to track dissemination of policies and procedures through employee attestation, as this provides a valuable input into policy enforcement and education processes.

Risk assessments play a crucial role in identifying potential threats to the organization and provide a perfect opportunity to implement effective controls to protect critical processes and assets. To support this, well-documented and high-quality information security policies, emphasized on the organization's commitment to conducting periodic (i.e. at least on an annual basis or as per business and technology needs) reviews as part of their overall risk management process (ISO/IEC 17799:2000/27002:2005) need to be implemented. In addition, an

organization should also develop an approved policy exception process, which essentially allows for risk based exemptions from policy where needed by a managed business purpose.

One of the key success factors in analyzing and measuring the effectiveness of information security is to ensure that the organization has a thorough understanding of the assets which are most valuable to them, and those assets have been allocated an appropriate level of data classification based on roles/responsibility, sensitivity and criticality of the asset relative to prioritized risk. The organization should also develop a set of procedures and provide specific training in relation to the information labeling and handling practice. It has become increasingly evident that organizations that do not have an approved and regularly communicated data classification policy have been the most vulnerable, in terms of information leakage.

Several years of research from various information security experts have revealed that people still are, and will always be, the weakest link when it comes to organizational security (ISO/IEC 17799:2000/27002:2005). Therefore, the organization's information security program will be an ineffective exercise/activity if an adequate level of information security awareness training for example corporate information security policies and procedures is not also implemented. Generally speaking, almost all security and privacy standards, frameworks, laws and regulations require organizations to educate their personnel in as part of overall policy and security awareness.

Security responsibilities should be captured in job descriptions and within terms and conditions that encompass employees, contractors and third parties. This ensures that they understand their responsibilities; are suitable for the role/contract they are being considered for; and reduces the risk of fraud, theft or misuse of assets and information processing facilities (ISO/IEC 17799:2000/27002:2005). There should also be a sanctions policy in place, which essentially describes the specific consequences of not adhering to the corporate policies and procedures. Even though sanction policies have not been widely adopted, they should be considered as a best-practice for effective information security management.

It is highly recommended when mapping access control rules and rights, that both logical and physical access be considered simultaneously – however, at the very least, information security policy should specify the requirements for logical access controls (including networks, operating systems, software applications and mobile devices) to effectively manage information

processing facilities as per business needs (COBIT, 2005). The logical access controls are the first to be developed and adopted by most organizations as they are related to human interaction with other security controls, for example the creation of user ID and passwords, and rights/privilege management). Without proper logical access controls, the organization may potentially be vulnerable to security incidents or increased technology risk.

One of the most commonly overlooked and poorly managed security domains is that of appropriate security controls over physical information processing infrastructure. The organization's information security policies should encompass physical and environmental security to ensure that all sensitive assets and processing facilities are secured, and protected by defined security controls linked to business risk.

Information security policy should specify all requirements and procedures throughout the information management lifecycle to minimize unauthorized disclosure, modification, removal and destruction of data, and to reduce interruption to business activities (COBIT, 2005). This can be accomplished by correctly labeling all critical data and information assets including paper and digital media, to define an appropriate level of protection and handling practice. This must be followed by appropriately protecting the asset during both storage and transmission, and destroying any aged or unwanted data in accordance with the information retention procedures. It should be noted that legislative or regulatory compliance may require organizations to retain certain types of data for a specified period, varying from several months to several years (US Privacy Act, 1974; Canadian Privacy Act, 1983; APEC Privacy Framework, 2004; EU Data Protection Directive, 1995; Fair Information Practices Act, 2010).

An appropriate level of maintenance is a critical part within any organization's overall information security program. The information security policies should address system acquisition, development and maintenance activities; including analysis of security requirements; ensuring data processing integrity and periodic review of enterprise applications; cryptographic controls; change management; and system files integrity (COBIT, 2005).

Over the past 5-10 years, privacy of both customers and employees has become the most talked-about issue within many organizations. It is interesting, yet alarming, that in today's modern technology driven society one of the fastest growing information crimes is identity theft, including customer data lost by organizations that were responsible for managing it. Such

incidents have emerged from all corners of the world, and have resulted in the introduction of strict national and international data protection laws in many countries, which require organizations to protect the personal information of stakeholders. Therefore applicable privacy laws and regulations must form a component of the organization's information security program (US Privacy Act, 1974; Canadian Privacy Act, 1983; APEC Privacy Framework, 2004; EU Data Protection Directive, 1995; Fair Information Practices Act, 2010).

Information security policies should address the communication, reporting, escalation and resolution of information security events and weaknesses, as differing events and weaknesses may adversely impact the security of organizations and even their partners or affiliates. System auditing, availability statistics, and performance metrics, provide vital information to assist in the evaluation and monitoring of incidents and potential vulnerabilities. This data can then be utilized for work plan validation or even forensics analysis following an incident or serious breach. The information security incident management procedure should be explicitly documented and all employees, contractors and third-parties should be educated in its requirements and their associated responsibilities (ISO/IEC 17799:2000/27002:2005).

Business continuity management must also form an integral part of any organization's information security policy, to support the continuity of critical business functions in the event of an incident, for example information system failures, and natural disasters. In the past, many organizations considered continuity management as a low-priority issue, the dramatic and publicized increase of business continuity related incidents such as natural disasters, wars and recent terrorist attacks, all around the world, have resulted in a rapid reevaluation of continuity risk at the executive level. An ever increasing number of organizations across the world are developing comprehensive business continuity processes and solutions to mitigate the impact of such events on their organization; and to improve their ability to rapidly adapt to changing circumstance via resilient policy and infrastructure designs, based on their organizational risk profile and business requirements (COBIT, 2005).

The business impact assessment process is another key component of overall business continuity, and should identify, analyze and evaluate the critical functions performed within the organization, including operational, financial, reputational and physical continuity requirements. Business continuity plans must be developed, and implemented to ensure timely resumption of

critical business functions. Furthermore, the business continuity plans should be tested periodically to ensure provision of appropriate roles and responsibility delegation, testing also provides an opportunity to evaluate new threats or adapt existing planning. Therefore, organisations which do not have proactive business continuity management may potentially be at risk of complete or partial disruption in the event of a continuity incident, this should be considered in the light of the fact that 90% of businesses cannot recover from a 2 week loss of financial data or financial operational capability.

Today's organisations encounter many different risks within their operational setting, however over the last decade; there has been one fundamental risk which has concerned the majority of fortune 500 companies. What is the potential risk of being sued or fined by a regulatory body? As almost all organisations must comply with some sort of legal requirements. Organisations should endeavour to obtain professional advice on all legal compliance matters from qualified and appropriately experienced legal practitioners, as legal requirements may vary from one country to another, for example trans-border flow of personal and customer information, and intellectual property rights. Therefore, an organisation's information security policies should encompass compliance with all necessary legal requirements to mitigate potential non-conformance, or breach of applicable laws, regulations or obligations (ISO/IEC 17799:2000/27002:2005).

2.2. Ensure clear alignment of the organization's information security activities with strategic business and technology activities

Fostering and continuously driving a security culture, and recognizing it as one of the single most critical core competencies within an organization will almost certainly assist any organization in becoming one step closer to their business goals. Misalignment between the information security activities, and strategic business requirements, may potentially result in a variety of adverse impacts across the organization. This misalignment is one primary reason why a number of the world's leading global organizations appear to not fully comprehend or realize significant improvement within their information security programs despite allocating significant budgets and highly skilled resources with ambitious agendas. It is clear that the organizational culture is a key contributor to this misalignment (COBIT, 2005).

The majority of technology-focused organizations expend enormous financial resources in the design, development, deployment and maintenance of cutting-edge enterprise security solutions. Yet despite such expenditure, they are still unable to clearly demonstrate any improvement across information security. For example, an organization's IT department had invested in excess of $700K in deploying a world-class Intrusion Detection System (IDS), but failed to consider the specific business security requirements.

2.3. Obtain appropriate levels of executive sponsorships, and establish strong governance structures within the organization

For any information security program to be effective, it is imperative that the executive and senior management not only have a reasonable understanding, but are committed to supporting the program through its lifecycle. It is recommended that executives and senior management should have a clear understanding of the organization's internal and external context, including stakeholders, culture, information system, legal and regulatory requirements, governance structure, values, history of events, security, compliance, audit, change management, standards, policies, procedures, financial and environmental influences. With such an understanding they can cascade this knowledge throughout the businesses.

To support this, a defined and well documented role and responsibility matrix should be developed, it should include reporting and communication channels for all participants within the information security program, ensuring both accountable and sustainable governance (COBIT, 2005). Without an appropriate level of executive sponsorship or the absence of authoritative governance structures, the information security program will be at risk of not achieving the defined security requirements or adequately addressing corporate informational risk.

2.4. Establish documented business and technology processes, and classify all organizational assets

Although skilled personnel are regarded as a critical requirement for organizational success, it is recommended not to undermine the importance of two additional factors, i.e. documented business and technology processes and the classification of all organizational assets. Both of these greatly assist the organization in effectively performing organizational information security activities. Although there are many benefits of process documentation, one of the most

advantageous is that they describe a sequential and systematic approach to conducting and completing business activities. Generally speaking, any given business process is accompanied by a specific objective which ultimately is aligned to the organization's mission and objectives. In the case of critical processes, their objective is far much more important as they substantially contribute towards the achievement of organizational operations, as such; a disruption in these processes has the potential to adversely impact operation. Organizational assets are items of great importance or value to the organization, which may come in many forms, such as corporate policies, procedures, personnel, systems, or even documentation. The most critical assets from an information security perspective are those that are required by critical processes (ISO/IEC 17799:2000/27002:2005).

2.5. Analyze current-state of organizational information security, and clearly define a realistic target-state

A majority of the organizations are very familiar with current-state security activities, but one of the most interesting yet challenging obstacles is to define a realistic target-state for their information security program. The target security state will vary from one organization to another; however in general, a target-state can be described as successfully satisfying information security requirements of critical processes and critical assets. It should also be noted that, establishing the target security state for any organization, regardless of their industry, is a multi-faceted and an extremely complex activity, as an organization's security expectations and requirements are often dynamic in nature. For example, an organization's IT department had deployed a multi-million dollar integrated financial management system, which warranted a review of information security, due to the associated criticality change. Therefore, this dynamic target-state demonstrates that today's organizations must be agile, responsive, flexible and themselves, dynamic, when it comes to establishing their security objectives, and driven by an overall need for continuous improvement.

2.6. Implement effective internal controls across the organization

One of the most important questions any internal or external auditor would ask is related to the level of internal controls within an organization. Most auditors are concerned with verifying that the internal controls within an organization are performing as expected, i.e.

controls are in place, are designed appropriately, are operating effectively, and are monitored regularly, in an effort to reduce risk exposure (COBIT, 2005). From an information security management perspective, internal controls are implemented to reduce risk associated with the execution of business processes to an acceptable level, set by executive management following a business impact assessment. When a business process is operating as expected, it is contributing to the organization's goals and objectives, and it also provides reasonable level of assurance to senior management over the integrity of its execution. For example, an organization's accounting and finance department received a purchase order to paying an IT vendor. Now, in the absence of appropriate controls, this could have result in either no payment, late payment, over payment or even a duplicate payment. Each of these could potentially result in a variety of adverse impacts, for example financial exposure, brand damage, refusal of supply. Therefore, effective internal controls must be established across the organization to satisfy security requirements over critical processes and assets.

3. Globally recognized international standards and frameworks

Today there are far too many standards and frameworks proprietary and non- proprietary available when it comes to managing information security, which is causing organizations to struggle in their selection and adoption of an appropriate security framework. To effectively create a solid foundation for an information security program, organizations need to analyze and implement their methodology in alignment with either of the following international standards and frameworks.

3.1. A brief overview of ISO/IEC 17799:2000/27002:2005 Information Technology Security Techniques – Code of Practice for Information Security Management

ISO/IEC 17799 is also known as ISO/IEC 27002, and provides practical guidance for initiating, implementing, maintaining and improving information security management practice, and facilitates confidence in inter-organizational information collaboration. The standard comprises eleven information security control domains, namely security policy; organisation of

information security; asset management; human resources security; physical and environmental security; communications and operations management; access control; information systems acquisition, development and maintenance; information security incident management; business continuity management; and compliance. Each of the eleven clauses contains control objectives which focus on what needs to be achieved, and one or more controls which focus on how to specifically achieve a given outcome. Lastly, it also contains specific 'implementation guidance' which provides detailed supporting information towards the effective implementation of control objectives (ISO/IEC 17799:2000/27002:2005).

3.2. A brief overview of Control Objectives for Information and related Technology (COBIT)

The internationally recognized Control Objectives for Information and related Technology (COBIT) is an IT governance framework, and provides process-driven guidance for initiating, implementing, maintaining and improving information technology security. The framework comprises four domains; namely plan and organize; acquire and implement; deliver and support; and monitor and evaluate. The four domains contain a total of thirty-four processes which provide a comprehensive end-to-end view business and technology across the whole security lifecycle (COBIT, 2005).

4. Conclusion

Organizational information security programs must be designed to assist organizations in identifying, adopting, and improving information security practice, in order to ensure that the organization can sustainably protect its business environment by creating a security culture based on the business rather than a traditional technologist centric environment. Effective information security programs highlight the development, communication, and publication of endorsed information security policies; and ensure a comprehensive understanding of the current-state security, while driving towards a realistic and business based target-state.

Ensuring alignment of the information security and strategic business direction; through executive sponsorship, and clearly defined governance practice is also vital to the effective implementation of any security program. Finally, the development of detailed process

documentation with careful classification of all information assets; ensures the effective and appropriate implementation of internal controls across the organization. Without these attributes, organizations will always have disparity and strategic misalignment within their information security program.

5. References

ISO/IEC 17799/27002 Information Technology Security Techniques, Code of Practice for Information Security Management; published by International Standardization for Origination (ISO). Website: http://www.iso.org

Control Objectives for Information and related Technology (COBIT) Frameworks 4th Edition; published by Information Systems Audit & Control Association (ISACA). Website: http://www.isaca.org

Fair Information Practices Act; published by United States Federal Trade Commission. Website: http://www.ftc.gov

U.S Privacy Act; published by Social Security Online. Website: http://www.ssa.gov

Canadian Privacy Act; published by Office of the Privacy Commissioner of Canada. Website: http://www.priv.gc.ca

APEC Privacy Framework; published by Asia-Pacific Economic Cooperation Secretariat. Website: http://www.apec.org

E.U Data protection Directive; published by European Commission. Website: http://ec.europa.eu