Journal of Executive Education

Volume 11 | Issue 1 Article 6

July 2013

Information Security Governance for the Non-Security Business Executive

Michael E. Whitman
Kennesaw State University, mwhitman@kennesaw.edu

Herbert J. Mattord
Kennesaw State University, hmattord@kennesaw.edu

Journal of Executive Education, 11(1) (2012). pp. 97–111

Information Security Governance for the Non-Security Business Executive

Michael E. Whitman*
Herbert J. Mattord
Kennesaw State University

Abstract

Information security is a critical aspect of information systems usage in current organizations. Often relegated to the IT staff, it is in fact the responsibility of senior management to assure the secure use and operation of information assets. Most managers recognize that governance is the responsibility of executive management. The primary objective of governance can be achieved when the members of an organization know what to do, how it should be done, as well as who should do it. The focus on governance has expanded to include more aspects of the organizational hierarchy to include information systems and information security. This article offers value to the executive by first defining governance as it is applied to information security and exploring three specific governance-related topics. The first of these examines how governance can be applied to the critical aspect of planning both for normal and contingency operations. The next topic describes the need for measurement programs and how such metrics can be developed for information security assessment and continuous improvement. Finally, aspects of effective communication among and between general and information security managers is presented.

*Dr. Michael Whitman is the Director of the Center for Information Security Education and Professor of Information Security; Dr. Herbert Mattord is the Coordinator of the Information Security and Assurance (ISA) Program and Assistant Professor of Information Security, both at Kennesaw State University.

Introduction

Governance has become a touchstone for those assessing organization's executive management over the past decade. Managers at every level recognize that governance is the responsibility for executive management to oversee the definition of expectation, distribution of authority and responsibility and the validation of performance within the organization. This fundamental aspect of good management has moved down the hierarchy from the Board Room to descending levels of the company's structure. Now, Information Technology (IT) management teams as well as Information Security (InfoSec) management teams are expected to implement the elements of good governance. It remains a primary responsibility of the organization's executive management to ensure that these technical departments are performing in the best interests of the organization, without getting ensnared in the details and minutia of the technical aspects which these groups are well known. It remains the executive's role to define expectations, provide and organize the resources and measure performance. These critical success factors can best be accomplished with carefully considered implementations of governance.

This paper outlines the responsibilities and duties of executive management with regard to the oversight of the Information Security function. This can ensure that those business functions comply with, and enable the normal and expected operations of the organization.

Overview of Information Security Governance

Information Security is the protection of the lifeblood of the organization — its information. Specifically it is the protection of the confidentiality, integrity and availability of that information and the systems that store, process and transmit it. Governance of this program and its core functions requires that senior executives be fully versed in the two disparate phases of strategic planning used by Information Security management and the processes used for the collection and reporting of measures that reveal performance.

Governance is "setting clear expectations for the conduct (behaviors and actions) of the entity being governed" (Allen, 2005). This encompasses the usual management functions such as controlling and directing the organization to influence the operational readiness of the organization. This also includes the specification of how organizations make critical

decisions including who makes decisions and who is accountable for outcomes. As with all management processes the desired outcome is the structuring of processes that produce consistent favorable results. Executives rely on subordinate managers to routinely make sound decisions that conform to management's intent as communicated in policy. Allen noted that "governance is most effective when it is systemic, woven into the culture and fabric of organizational behaviors and actions" (2005). When developed and implemented properly governance will instantiate and maintain a fabric of policy, informed by principle that makes processes effective. InfoSec governance is management's obligation to assure that the organization achieves its business objectives and delivers value for the stakeholders (Spokes & Worstell, 2009). Spokes and Worstell also observed that in order for governance to "establish a solid base for a defensible standard of due care and demonstrate due diligence to that defensible standard" (2009), it is crucial to clearly define and assign responsibilities for the organizational members with various responsibilities in the area.

According to the Corporate Governance Task Force — an alliance of industry and government sectors — the oversight of an organization's strategy for implementing information security includes: "Understanding the criticality of information and information security to the organization, reviewing investment in information security for alignment with the organization strategy and risk profile, endorsing the development and implementation of a comprehensive information security program and requiring regular reports from management on the program's adequacy and effectiveness" (ITGI, 2006).

In order for InfoSec Governance to be considered effective, the organization must "demonstrate a set of beliefs, behaviors, capabilities and actions that consistently indicate that an organization is addressing security as a governance concern:

- Security is enacted at an enterprise level.
- Security is treated the same as any other business requirement.
- Security is considered during normal strategic and operational planning cycles.
- Security is integrated into enterprise functions and processes.
- All personnel who have access to enterprise networks understand their individual responsibilities with respect to protecting and preserving the organization's security condition" (Allen, 2005).

Implementing and Maintaining Governance for the Organization

The first step in establishing effective governance strategy for the organization is the establishment of an implementation methodology — a formal approach to the design, development and implementation of the strategy. While some organization may be well versed in Corporate or IT Governance, the concept of InfoSec Governance is new enough, and different enough, to warrant an examination of the approach to effective and efficient methodology use.

In order for a new InfoSec Governance strategy to be effective the organization must first establish a governance structure for Information Security. Since the roles and responsibilities of the Chief Information Officer (CIO) and the Chief Information Security Officer (CISO) may at times be at odds, it is generally not recommended to simply funnel the governance of InfoSec through an established IT Governance structure, if one exists. As the CIO is primarily responsible for the efficiency of information processing, and the inherent nature of InfoSec in protecting that information tends to retard that efficiency, it is generally advised to separate the two governance structures. In addition, the CISO must seek to support, not only the functions and operations of the IT department in its information protection strategies, but also those of the rest of the organization — as every business unit contains information assets in various forms on which the entire organization relies on for efficient and effective operations.

The preliminary tasks in establishing an InfoSec Governance structure include the following, as specified by ISACA's *Implementing and Continually Improving IT Governance* document (ISACA, 2009) are as follows:

Identify the Stakeholders - The first task is to identify those groups that will have a vested interest in the governance structure and who may be directly involved. These groups include: Executive management Business management and business process owners Chief information officer (CIO), IT management and IT process owners IT audit Information Security including Risk and compliance.

Define the Governance Board - Once the stakeholders are identified, those that should, and are willing to, serve on a governance board should be identified. Once identified, their primary roles and responsibilities should be defined. According to ISACA, these roles include the following:

- **Board and executives** - Set direction for the program, ensure alignment with enterprise-wide governance and risk management, approve key program roles and define responsibilities, and give visible support and commitment. Sponsor, communicate and promote the agreed-upon initiative
- **Business management** - Provide appropriate stakeholders and champions to drive commitment and to support the program. Nominate key program roles and define and assign responsibilities
- **IT management** - Ensure that the business and executives understand and appreciate the high-level objectives. Nominate key program roles and define and assign responsibilities. Nominate a person to drive the program in agreement with the business
- **IT audit** - Agree on the role and reporting arrangements for audit participation. Ensure that an adequate level of audit participation is provided through the duration of the program
- **[Information Security] Risk and compliance** - Ensure an adequate level of participation through the duration of the program (ISACA, 2009).

Review the Key Success Factors - A key success factor, or critical success factor, is something that must go right for the operation to succeed. Absence of these factors can substantially decrease the probability of success in the venture. For IT (and InfoSec) governance, the key success factors are: Top management investiture: More than simply a memo from top management, executive management must demonstrate investiture in the governance structure by meeting and establishing the direction and purpose (mandate) for the governance function. They must demonstrate to the entire organization that they are dedicated to the process. These factors are:

- Understanding of the outcomes and objectives: In addition to understanding the impetus of the governance function, all stakeholders in the process must understand WHY the governance is being done, the business, IT and InfoSec objectives and desired governance outcomes.
- Implementing effective change management: In order for any change to be effective and established as new organizational culture, the projected changes to result from the governance effort must be clearly communicated and then enabled

- Customization of the governance framework to the organization: A careful adaptation of any governance framework is required to ensure it meets the needs and ability of the organization. The tailoring of the practices and procedures must be carefully effected to maximize compatibility
- Pick the low hanging fruit first: The project should look for activities that can be quickly implemented with clear benefits realized. Identify those components of the governance project, like an executive briefing on InfoSec issues in the cloud that can be easily and quickly performed, with immediate results realized (ISACA, 2009).

Adopt a Governance Implementation Methodology - A methodology promulgated by groups such as ISACA can be used to initiate the Governance function (ISACA, 2009). Steps in such a program might include:

- Begin the program development process to find and articulate what business activities cause change and how the desires for change are converted into policy and process change directives. This should be done with a formal business case that spell out the risks and how they might be controlled. These change drivers might include a variety of events or actions inside and outside of the organization including change in the legal and regulatory environment, market competition, technical evolution , performance failures, or revision of the goals of executive management.
- Explicitly identify the problems to be solved and/or the opportunities to be seized. This is best achieved with a process that seeks to align the IT and Information Security objectives to those from the business units being supported. These should be presented using a priority-based approach that uses a model like COBIT that can help gain some assurance all relevant factors are being considered and that all necessary processes have been defined, managed and controlled. The intent is to identify current capabilities and then point out the gaps that might exists between the current state and the desired future state.
- Plan out the steps necessary to reach that objective. Using the prioritized objectives from the prior step, set a sequence of objectives to form a roadmap for improvement. Some of the objectives will

be quickly achieved and others may take longer. Those longer that you think are reasonable for your organizational culture should be divided into more manageable objectives. Priority should be awarded to those projects that are easiest to achieve and will have the most beneficial result.
- Prepare a business case and project plan for each objective.
- Using your organization's established project management processes (or those you choose to adopt for these projects), execute your plans. This should involve both the implementation of the proposed solutions and the creation of measures and processes to monitor progress and gain assurance that the projects are well aligned to business objectives, and stay that way.
- Assess each project in the process to determine if the initial objectives were achieved. One measure of success will be the degree to which the new processes are integrated into the normal business operations of the organization. Once again, the use of measures and assessments are essential to make certain the necessary progress is reached and retained.
- Finally, review the objectives with an eye toward keeping the improvement program moving forward and recognizing the need for ongoing and continuous security program improvement.

Aspects of Security Governance: Strategic Planning for Normal and Contingency Situations

It is difficult to overstate the essential nature of strategic planning in business and organizational management. As President Dwight D. Eisenhower stated, "plans are useless, but planning is invaluable" (1957). Information security strategic planning involves some aspects of planning common to the entire organization. The establishment of a mission, vision and values statement, the establishment of long term goals and objectives, and the development of strategic plans to be translated into tactical and operational plans and operations. This part of information security governance should be familiar to the organization's top management. Another aspect of InfoSec strategic planning may not. Because the information security function influences and affects the entire organization, an effective information security executive should know how to integrate the InfoSec strategic planning into the organizational planning process works so that the plans can yield measurable results.

InfoSec Strategic Planning for Non-Normal Business Operations

A critical part of the strategic planning that InfoSec executives are expect to contribute to involves those plans targeted for non-standard operations — the contingency planning function. While InfoSec may not be the dominant planner or player in such a planning endeavor, they are a critical one. The need to have a plan in place that systematically addresses how to identify, contain, and resolve unexpected events has been around as long as IT. When an unexpected event occurs, the organization must have policies, plans and procedures in place that will allow it to continue critical and essential operations, even if IT support is interrupted (Swanson et al, 2006). Some organizations — particularly government agencies — are charged by law or other mandate to have such procedures in place at all times.

The development of plans for handling unexpected events should be a high priority for all executives, both Information Security and Business: Corporate and InfoSec Governance demands it. The overall process of preparing for unexpected events is called contingency planning (CP). CP is the process by which the IT, InfoSec and Corporate business functions prepare for, detect, react to, and recover from events that threaten the security of information resources and assets, both human and natural. "The main goal of CP is to restore normal modes of operation with minimal cost and disruption to normal business activities after an unexpected event — in other words, to make sure things get back to the way they were within a reasonable period of time. Ideally, CP should ensure the continuous availability of information systems to the organization even in the face of the unexpected" (Whitman & Mattord, 2010).

CP consists of four major components, the Business impact analysis (BIA), Incident response plan (IR plan), Disaster recovery plan (DR plan) and Business continuity plan (BC plan). The BIA, a preparatory activity common to both CP and risk management, helps the organization determine which business functions and information systems are the most critical to the success of the organization, enabling subsequent plans to focus on those functions and systems. The IR plan focuses on the immediate response to an incident. Any unexpected event is treated as an incident, unless and until a response team deems it to be a disaster. Then the DR plan, which focuses on restoring operations at the primary site, is invoked. If operations at the primary site cannot be quickly restored — for example, when the damage is major or will affect

the organization's functioning over the long term — the BC plan occurs concurrently with the DR plan, enabling the business to relocate to and establish operations at an alternate site, until the organization is able to resume operations at its primary site or select a new primary location.

Depending on the size and business philosophy of an organization, information technology and information security managers can either (1) create and develop these four CP components as one unified plan or (2) create the four separately in conjunction with a set of interlocking procedures that enable continuity. Typically, larger, more complex organizations create and develop the CP components separately, as the functions of each component differ in scope, applicability, and design. Smaller organizations tend to adopt a one-plan method, consisting of a straightforward set of recovery strategies.

Ideally, the CIO, systems administrators, CISO, and key IT and business managers should be actively involved during the creation and development of all CP components, as well as during the distribution of responsibilities among the three communities of interest. The elements required to begin the CP process are: a planning methodology; a policy environment to enable the planning process; an understanding of the causes and effects of core precursor activities, known as the BIA; and access to financial and other resources, as articulated and outlined by the planning budget. Each of these is explained in the sections that follow. Once formed, the contingency planning management team (CPMT) begins developing a CP document using the following process:

1. Develop the contingency planning policy statement: A formal department or agency policy provides the authority and guidance necessary to develop an effective contingency plan
2. Conduct the BIA: The BIA helps to identify and prioritize critical IT systems and components (see NIST Special Publication 800-34, Rev. 1)
3. Identify preventive controls: Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs
4. Develop recovery strategies: Recovery strategies ensure that the system may be recovered quickly and effectively following a disruption
5. Develop the contingency plan: The contingency plan should contain detailed guidance and procedures for restoring a damaged system

6. Conduct plan testing, training, and exercises: Testing the plan identifies planning gaps, whereas training prepares recovery personnel for plan activation; both activities improve plan effectiveness and overall agency preparedness
7. Maintain the Plan: The plan should be a living document that is updated regularly to remain current with system enhancements.

Effective contingency planning begins with effective policy. Before the CP team can fully develop the planning document, the team must first receive guidance from the executive management, as described earlier, through formal contingency planning policy. This policy defines the scope of the CP operations and establishes managerial intent in regard to timetables for response to incidents, recovery from disasters, and reestablishment of operations for continuity. It also stipulates responsibility for the development and operations of the CP team in general and may also provide specifics on the constituencies of all CP-related teams.

The CP team (or Contingency Planning Management Team — CPMT) collects information about information systems and about the threats they face, conducts the business impact analysis, and then creates the contingency plans for incident response, disaster recovery, and business continuity. The CP team often consists of a coordinating manager and representatives from each of the other three teams, as well as representatives from the business areas to be supported. As indicated earlier, in larger organizations the IR, DR and BC teams are distinct entities, without overlapping membership, although the latter three teams have representatives on the CP team. In smaller organizations, the four teams may include overlapping groups of people.

Many organizations' contingency plans are woefully inadequate. CP often fails to receive the high priority necessary for the efficient and timely recovery of business operations during and after an unexpected event. The fact that many organizations do not place an adequate premium on CP does not mean that it is unimportant, however. The Computer Security Resource Center (CSRC) at the National Institute for Standards and Technology (NIST) recommends these procedures (contingency plans, business interruption plans, and continuity of operations plans) should be coordinated with the backup, contingency, and recovery plans of any general support systems, including networks used by the application.

Performance Measures: Governing Success

The use of performance measures in business is certainly not a new thing, however the use in assessing and communicating the effectiveness of the information security program is. It is important for the sake of InfoSec governance for the executive management to expect quality in performance measures (also known as metrics), and ensure that the information being conveyed is suitable to indicate the relative success of the InfoSec program. While some managers may assert that the costs, benefits and performance of InfoSec are almost impossible to measure, in fact they are measurable; doing so requires the design and ongoing use of an InfoSec performance management program based on effective performance metrics. This is not to infer that InfoSec should be treated as a profit center. In fact the benefits of a highly effective InfoSec program are counter-intuitive. The ideal state of a highly effective InfoSec program would appear from the outside as a waste of funding. The employees would be underworked, with seemingly little to do, primarily because their work would be so effective as to negate any attack on the organization's information. InfoSec's primary mission is to be invisible yet so effective as to halt any attack before it effects the organziation, making sure the organization's information is available whenever, wherever and however the users need it, without any fear of loss, modification or disclosure.

InfoSec Performance Management

This paper will presume that the executive reading it is already trained in the development and implementation of a performance measure program, thus leaving only the need to define what metrics within the realm of InfoSec should be defined and applied in order to effectively assess the success of the InfoSec function. If not, there are several suitable references available for the design and implementation of performance measures programs including the NIST Special Publication 800-55, Revision 1: Performance Measurement Guide for Information Security (Chew, Swanson, Stine, Bartol, Brown, & Robinson, 2009).

As was observed by Chew, et al. (2009), effective InfoSec management can be achieved when measures are chosen that can be used to measure the overall security program. They note that if data points can measure the effectiveness of the technical and/or managerial control regimes put in place, those who rely on the control regimes can then

make informed decisions about such control regimes. This might mean removing ineffectual controls to seek more effective replacements and the continuation of effective controls to maintain the desired result and achieve the desired effect.

Organizations typically use three types of measures:

- Those that determine the effectiveness of the execution of information security policy, most commonly issue-specific security policies to meet new information security requirements as they occur.
- Those that determine the effectiveness and/or efficiency of the delivery of information security services, whether they be managerial services such as security training, or technical services such as the installation of antivirus software
- Those that assess the impact of an incident or other security event on the organization or its mission (Chew et al., 2009).

Specifying InfoSec Metrics

One of the critical tasks in the measurement process is to assess and quantify what will be measured. While InfoSec planning and organizing activities may only require time estimates, you must obtain more detailed measurements when assessing the effort spent to complete production and project tasks. This usually means some form of time reporting system, either a paper-based or automated time accounting mechanism.

Production level statistics depend greatly on the number of systems and the number of users of those systems. As the number of systems changes and/or the number of users of those systems changes, the effort to maintain the same level of service will vary. Some organizations simply track these two values to measure the service being delivered. Other organizations need more detailed metrics, perhaps including the number of new users added, number of access control changes (adding, removing or modifying resource permissions), number of users removed or de-authorized, number of access control violations (such as failed login attempts or individuals attempting to access information they are not authorized to), number of awareness and training briefings, number of systems by type, number of incidents by category (such as virus or worm outbreaks), number of malicious code instances blocked by filters

(such as firewalls), and many, many other possible measurements.

A number of example candidate measures are listed here. Additional details on these measures, including how they are calculated and used, are provided in NIST SP 800-55, Rev 1.

These examples illustrate how an organization might begin measuring concrete outcomes from managerial programs in order to begin the process of assessing improvements made to information security programs a means of measuring improvements to governance processes:

- Percentage of the organization's information systems budget devoted to information security
- Percentage of high vulnerabilities mitigated within organizationally defined time periods after discovery
- Percentage of remote access points (e.g. WiFi routers) used to gain unauthorized access
- Percentages of information systems and general business personnel that have received security training
- Average frequency of audit records review and analysis for inappropriate activity
- Percentage of new systems that have completed certification and accreditation prior to their implementation
- Percentage approved and implemented configuration changes identified in the latest automated baseline configuration
- Percentage of information systems that have conducted annual contingency plan testing
- Percentage of users with access to shared accounts
- Percentage of incidents reported within required time frame by incident category
- Percentage of system components that undergo maintenance in accordance with formal maintenance schedules
- Percentage of media that passes sanitization procedures testing (cleaning drives prior to reuse)
- Percentage of physical security incidents allowing unauthorized entry into facilities containing information assets
- Percentage of employees who have signed policy compliance forms by policy
- Percentage of individual screened before being granted access to organizational information and information systems
- Percentage of system and service contracts that include security requirements and/or specifications

- Percentage of mobile computers and devices that use approved encryption modules
- Percentage of operating system vulnerabilities for which patches have been applied or that have been otherwise resolved (Chew, et al, 2009).

Effective Communications between Infosec and Executive Management

Whether it is the reporting of performance measures, or the presentation of InfoSec strategies and plans, two fundamental premises must occur in in order to meet the intent of industry-recognized processes for governance:

1. These efforts must occur and must occur as a collaboration of those that work in the field, and the top executive management. The organization cannot afford to risk a *filtering effect* where bad news is downplayed to make an individual manager or department look better. The cold, hard facts as measured must be presented in order for the top executives to fully understand the state of their organization.
2. Those working in technical fields like IT and InfoSec, must be forced to speak a common language of business, where specialized terminology and shared assumptions are either removed or carefully spelled out. There should be a fundamental expectation that all presentations will be developed in such a way as to be easily understood by top management, without the technical jargon and language that can easily obfuscate and hide the true status of the program.

Conclusion

Many organizations have already rethought how they can reduce the risk of using information systems. Of these, many have discovered that information security is a separate function from the information systems business unit. Whether it is achieved as part of the IT function or as part of another executive role, it is the responsibility of senior management to assure the secure use and operation of information assets.

Information security governance is achieved when those members of the organization charged with that responsibility know what to do, who is to do it, and how it should be done. When executive management fails to plan for success and does not design and implement highly functional governance structures and programs, information assets will be exposed to higher levels of risk and information used in the organization may be compromised and have reduced value.

References

Allen, J. (2005). Governing for enterprise security. *Carnegie Mellon University/Software Engineering Institute Technical Note CMU/SEI-2005-TN-023*. WWW document viewed 1/12/2012 from http://www.cert.org/archive/pdf/05tn023.pdf.

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., & Robinson, W. (2009). Performance measurement guide for information security. *NIST Special Publication 800-55, Revision 1*.WWW Document viewed 1/15/2012 from http://csrc.nist.gov/publications/nistpubs/.

Eisenhower , D. (1957). *Public papers of the presidents of the United States.* National Archives and Records Service, Government Printing Office, p. 818

ISACA. (2009). *Implementing and Continually Improving IT Governance Document*. WWW Document viewed 1/15/2012 from http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Implementing-and-Continually-Improving-IT-Governance1.aspx.

ITGI. (2006). *Information security governance: Guidance for Boards of Directors and Executive Management, Second Edition.* WWW Document viewed 1/15/2012 from http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/ Information-Security-Governance-Guidance-for-Boards-of-Directors-and-Executive-Management-2nd-Edition.aspx

Spokes, J. & Worstell, K. (2009). Governance in cloud and virtualized environments. *ISACA Webcast.* Retrieved August 10, 2010 from www.brighttalk.com/webcast/4078.

Swanson, M., Hash, J., & Bowen, P. (2006). Guide for developing security plans for federal information systems. *NIST Special Publication 800-18, Revision 1.* WWW Document viewed 1/15/2012 from http://csrc.nist.gov/publications/nistpubs/.

Whitman, M., & Mattord, H. (2010). Management of Information Security. Cengage/Course Technology.