DOI: 10.1145/1435417.1435446

BY ALLEN C. JOHNSTON AND RON HALE

Improved Security through Information Security Governance

WITHIN THE MODERN, HYPER-CONNECTED business landscape, organizations are constantly under attack. According to the 2005 Computer Crime and Security Survey, conducted jointly by the Computer Security Institute (CSI) and the San Francisco Office of the Federal Bureau of Investigation (FBI), 56% of respondents reported unauthorized computer system use during the past year.[2] These unauthorized uses include malicious acts such as theft or destruction of intellectual property, insider abuse and unauthorized access to information that results in a loss of data integrity and confidentiality, as well as malware threats such as viruses, spyware, worms, and Trojans.[2] Based on responses obtained from a sample of 700 security practitioners from government, financial, medical, business, and higher education institutions, the most frequently reported forms of malicious attack were virus attacks and insider abuse at a reported rate of approximately 75% and 50%, respectively.[2] Within the realm of the 639 respondents willing to estimate losses due to threats, the total costs associated with virus attacks were determined to be approximately $43 million, while insider abuse costs were nearly $7 million.[2] While these figures are an improvement over past years, clearly many firms still operate ineffective information protection programs.

Ineffective protection can often be attributed to the manner in which firms go about planning their information security programs.[6] Far too many firms take a reactive approach to information security planning.6 Their strategies for asset protection are derived from the bottom up, based on incidents at the perimeter of the organization. As such, these firms segregate information security from their overall strategic directive, thereby creating a divide between the governance of the firm and the management of information security. The results of such a disconnect can be disastrous, as management and employees may lose touch with the value of appropriate security actions and as business processes become bogged down with unnecessary or improper controls. In scenarios such as these, a different perspective for security planning is warranted.

In this article, we examine information security planning at the strategic level of the enterprise and empirically assess its value in enhancing the quality of information security programs. Included in this examination is a survey of security professionals in which they report their perceptions of information security program quality within their respective firms. The results of this study allow us to compare the quality of information security programs implemented as part of an enterprise-level governance process with those implemented outside of the enterprise governance process. Moreover, the results allow us to paint a picture of the value of aligning the goals of information security with those of the entire enterprise.

Information Security Governance

When we consider enterprise governance, we think of executive management actions that provide strategic direction to the firm, while achieving its objectives, ameliorating risk, and managing resources in the most effective and efficient manner possible.[1] On an enterprise level, planning leads to strategies which provide direction to the firm and touch on all aspects of the organization, including financial, research and development, marketing, human resource, and information technology resources. These strategies are reflected in the policies and procedures of the firm and are ultimately executed as part of the enterprise governance process—the set of activities that ensure a firm's strategies are implemented and policies executed.

Information Security Governance (ISG) is an essential element of enterprise governance and consists of the leadership, organizational structures, and processes involved in the protection of informational assets.[4] Through ISG, firms can address the issues of information security from a corporate governance perspective, thereby optimizing certain outcomes.[7]

Because ISG brings information security to the attention of Boards and CEOs, firms can more effectively and efficiently address the issues of information security leading to improved outcomes, including strategic alignment, risk management, business process assurance, value delivery, resource management, and performance measurement.[4] In terms of strategic alignment, ISG enables firms to align security with business strategy to support organizational objectives. Firms are also likely to execute appropriate measures to reduce risks and potential impacts to an acceptable level and integrate all relevant assurance factors to ensure processes operate as intended from end to end. ISG also supports the optimization of security investments in support of business objectives and enables the firm to use security knowledge and infrastructure in the most efficient and effective manner possible. Finally, ISG better enables the monitoring and reporting of security processes to ensure the achievement of objectives.

When information security is addressed as part of the strategic planning process, a firm's policies and procedures are more likely to include the goals and objectives of its desired information security posture.[4,7] This level of planning allows information security initiatives to be more seamlessly integrated with the overall goals and objectives of the organization, and in doing so lend them more significance. Also, when addressed at the strategic level, information security initiatives are more likely to be recognized and supported by executive management.

Table 1. Perceived Quality of Executive Mangement Support

Executive Management Support Indicator	ISG Implementers (mean/sd)	ISG Non-Implementers (mean/sd)	t-value
Executive management understand the relevance of information security to the organization	3.19/.715	2.29/.784	5.196
Executives promote effective information security governance	2.89/.816	1.57/.676	6.931
Executives actively support the information security program	3.04/.788	1.81/.814	6.493
Executives comply with all aspects of the information security program	2.66/.830	1.57/.676	5.627
Executive management understands their responsibility for information security	2.92/.818	1.76/.768	5.959
Executives understand the liability associated with not executing information security responsibilities	3.02/.805	2.05/.805	5.054

all findings significant at $p < 0.001$; sd = standard deviation

Measuring the Value of ISG

As a means of quantifying the value of an ISG program, a Web-based survey was conducted of business executives, information systems managers, security practitioners, consultants, and auditors who had been awarded the Certified Information Security Manager (CISM) certification by ISACA. The survey was anonymous as it did not require anyone to log on or to identify themselves in any way. Some 628 security professionals were contacted and asked to self-report their perceptions of the information security program quality in their current organization across a variety of outcomes, including executive management support, the relationship between business and information security, and information protection. A total of 151 (24%) usable, complete responses to this Web-based survey were received.

As part of the survey, respondents were asked to identify their role in their organization, industry, location, and industry affiliation. Since the CISM certification is intended for practitioners with information security management experience, almost all of the respondents reported being either directly responsible for providing information security management services or were executive and IT management with a background in information security. The largest grouping of survey takers (34.5%) were chief information security officers or had other positions in information security management. Executive management, who were certified in information security management but had a different role in their firms, accounted for 24.3% of survey respondents. The remaining 31% were accounted for in IT management (14.2%), consulting and service providers (18.9%) and others, all of whom were certified information security managers.

The majority survey participants (20.9%) worked in the financial services industry including banking, insurance, and investment services. The next largest organizational categories included federal, state, and local government which collectively accounted for 12.9% of survey participants. Most participants were from North America (53.4%) or Europe (21.2%). When examining the size of represented organizations, 56% of survey participants worked in organizations with more than 1,000 employees. Almost one third of the total survey sample was comprised of individuals from organizations with more than 10,000 employees. Small organizations with 50 or fewer employees accounted for 17.6% of the survey sample.

Survey participants were asked to report the degree to which they had implemented an ISG program. For this

Table 2. Perceived Quality of Business and Information Security Relationship

Relationship Indicator	ISG Implementers (mean/sd)	ISG Non-Implementers (mean/sd)	t-value
Security investments are optimized to support business objectives	2.70/.725	1.95/.805	4.220
Business process owners actively support the information security program	2.66/.892	1.57/.598	5.347
Business process owners view security as an enabler	2.50/.928	1.48/.680	4.819
Business process owners are involved in evaluating security alternatives	2.45/.804	1.62/.740	4.375
Business process owners actively support the development of a security culture	2.55/.860	1.48/.680	5.400
Business process owners accept responsibility for information security	2.50/.873	1.57/.598	4.625
Business process owners are accountable for information security	2.50/.920	1.38/.590	5.342

all findings significant at $p < 0.001$; sd = standard deviation

Table 3. Perceived Quality of Information Protection

Information Protection Indicator	ISG Implementers (mean/sd)	ISG Non-Implementers (mean/sd)	t-value
All information in use within the organization is identified	2.65/.829	1.76/.889	4.439
Information is classified according to criticality	2.78/.914	1.76/.768	4.758
Information is classified according to sensitivity	2.79/.953	1.80/.768	4.390
Information classifications are enforced	2.61/.991	1.52/.750	4.768
Information classifications are applied to information received from outside entities	2.59/.944	1.62/.669	4.509
Information classifications are applied to information provided to an outside entity	2.78/.945	1.95/.865	3.699
Ownership responsibilities for all information is assigned	2.70/.882	1.62/.669	5.323
Applications that process sensitive information are identified	2.95/.873	2.05/.805	4.400
Applications that support critical business processes are identified	3.10/.764	2.10/.889	5.377
Data retention standards are defined and enforced	2.70/.845	1.95/.921	3.624

all findings significant at $p < 0.001$; sd = standard deviation

study, participants employed within firms that had either executed an ISG program or were in the process of executing an ISG program are referred to as ISG Implementers. Conversely, participants working in firms that had neither executed an ISG program nor had considered such a program are referred to as ISG Non-Implementers.

Executive management support is frequently cited as a critical component for information security program success.[3, 8] As shown in Table 1, survey results indicated ISG Implementers self-reported significantly higher levels of executive management support quality than ISG Non-Implementers ($p < .001$ for all indicators). Scale endpoints for quality ranged from poor (1) to excellent (4). Perhaps highlighting this discrepancy was the differential in the degree to which ISG Implementers (3.04) and ISG Non-Implementers (1.81) perceive executives as actively supporting the information security program.

An implication of these findings is that ISG programs expose executive personnel to relevant information security issues, thereby facilitating an understanding of and commitment to information security. As executive managers, such as CEOs or CKOs, take a more active and supportive role in promoting information security, their influence is felt throughout the firm. The result is a culture in which secure computing practices are the norm rather than the exception and are engrained in the very processes that drive the organization.

The discrepancy of perceptions between ISG Implementers and ISG Non-Implementers also holds true for the relationship between business and information security. As shown in Table 2, ISG Implementers perceived significantly stronger relationships between business and information security than their ISG Non-Implementer counterparts ($p < .001$ for all indicators). The greatest differential in perspectives concerns the degree to which ISG Implementers and ISG Non-Implementers view business process owners as actively supporting the development of a security culture (t-value = 5.400).

These findings suggest that when information security is addressed at the corporate level as part of the enterprise planning process, it is afforded greater ownership by employees of the firm. Greater ownership means that employees are more responsible and accountable for the security of their assets, and view security not as a barrier to success, but as an enabler. Improved ownership also contributes to an organizational culture of secure computing.

ISG Implementers also reported significantly ($p < .001$ for all indicators) higher levels of information protection quality than ISG Non-Implementers. As displayed in Table 3, ISG Implementers reported consistently higher levels of protection quality across a number of critical indicators including information identification (t-value = 4.439), information classification based on criticality (t-value = 4.758), information classification based on sensitivity (t-value = 4.390), information ownership responsibilities (t-value = 5.323), and data retention standards (t-value = 3.624).

The differential in perspectives between ISG Implementers and ISG Non-Implementers has several likely sources, including more involved executive management, a more supportive organizational culture, and a general population of employees with a greater sense of ownership and responsibility

for the protection of their information assets. These are issues of awareness and preparedness.[5, 6] Implications are that ISG Implementers are more aware of threats to information security and better prepared to deal with the threats should they become an attack reality.

Further analysis reveals that for each of the reported measures of quality, the differentials in the minimum and maximum values are greater for ISG Non-Implementers than for ISG Implementers. This implies that ISG Implementers view each scale item as an important condition toward successful information protection, with less variation in their perspectives than ISG Non-Implementers. Moreover, the greater variance in the responses provided by ISG Non-Implementers suggests a lack of awareness of critical security indicators and a general lack of consistency in their approach to information protection.

Motivation for ISG

The results of this study lend support to the inclusion of information security planning as part of the enterprise governance process, thereby aligning security with other core business assets and processes critical to the success of the firm. Yet, for some firms there may be barriers in place that provide resistance to the development of an ISG program. For instance, when information security is seen only as an operational component of information technology it may be difficult for management outside of IT to contribute to or support information security initiatives or to build a case for information security program value. This wider view and participation in information security program strategies and activities is an essential component of information security governance.

There are numerous incentives for initiating an ISG program. ISG Implementers were asked to rate the level of influence of various factors on their decision to implement an ISG program. With influence scale endpoints ranging from low (1) to high (5), legal requirements (4.30) were the most influential factor, closely followed by government regulations (4.24). All survey respondents were then asked to rate the importance various factors would have in providing motivation to implement an ISG program. With the scale endpoints for importance ranging from low (1) to high (5), concerns over civil and legal liability (4.20) was considered the most important factor, followed closely by the protection of the organization's reputation (4.19) and compliance with regulatory initiatives (4.00).

Limitations

While the findings of this research are certainly promising and point to a clear incentive for ISG program implementation, there are some limitations. One such limitation lies in the classification or grouping of ISG Implementers. Those that had either executed an ISG program or were in the process of executing an ISG program were classified as ISG Implementers, leaving those that had neither executed an ISG program nor considered such a program to be classified as ISG Non-Implementers. While this grouping provided for an interesting macro-level analysis of the influence of ISG programs, future research should investigate differences in perspectives among the various levels of implementers and non-implementers. Additionally, future research should more closely examine the maturity of ISG implementation – contrasting the perspectives of new implementers involved in the early stages of implementation against those with established ISG programs.

Finally, it could be argued that the perspectives of a sample consisting entirely of CISMs are limited. However, in order to gauge the effectiveness of ISG programs in improving the quality of information programs, CISMs are perhaps the best authority. Their position within the firm, as implementers of the ISG initiatives, provides them which a unique insight into the effectiveness of their program. Future research, however, should capture the perspectives of the various stakeholders within the firm. Contrasting these perspectives with those of the CISMs would make for an interesting study.

Conclusion

Given the critical nature of a firm's information, organizations must be proactive in their approach to information security. This study provides empirical evidence in support of an ISG program as an important condition for the success of an information security program. It also adds support for the concept that information security provides benefits to firms when addressed as an enterprise issue and integrated into executive planning and strategy. While an ISG program may be approached by some organizations as part of a regulatory compliance strategy, the advantages to firms are wider in terms of supporting organizational objectives and effectively managing risk.

For those firms that are able to implement an ISG program, the evidence provided by this study suggest that they will enjoy improved information security in terms of the quality of executive management support, the relationship between business and information security, and information protection. Considering these benefits, the question becomes: Why aren't all firms currently engaged in ISG implementation? While the majority of the respondents of this study point to legal requirements or regulatory compliance as reasons for ISG implementation, there are many factors that influence such action. Certainly, concerns of civil and legal liability, the reputation of the firm, and compliance with regulator initiatives serve as legitimate influential factors. Yet for all of these motives, isn't the promise of improved security reason enough? C

References

1. CIMA/ IFAC. Enterprise governance: Getting the balance right. www.cimaglobal.com/downloads/enterprise_governance.pdf, (Jan. 11, 2005).
2. Gordon, A. L., Loeb, P. M., Lucyshyn, W., and Richardson, R. 2005 CSI/FBI computer crime and security survey. *Computer Security Institute* (2005), 1-26.
3. Hambrick, D. C. and Mason, P. A. Upper echelons: The organization as a reflection of its top managers. *Academy of Management Review* 9, 2, (1984), 193-206.
4. IT Governance Institute. Information security governance: Guidance for boards of directors and executive management. www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=24572. (July 7, 2006)
5. Siponen, M. T. A conceptual foundation for organizational information security awareness. *Information Management & Computer Security 8*, 1 (2000), 31-41.
6. Straub, D. W., and Welke, R. J. Coping with systems risk: Security planning models for management decision making. *MIS Quarterly 22*, 4 (1998), 441-469.
7. Warkentin, M., and Johnston, A. C. IT governance and organizational design for security management. Chapter 3 in Baskerville, R., Goodman S., and Straub, D. W. (Eds.). *Information Security Policies and Practices*, M.E. Sharpe, 2006.
8. Whitman, M. E. Enemy at the gate: Threat to information security. *Communications of the ACM 46*, 8 (2003), 91-95.

Ron Hale (rhale@isaca.org) is a certified information security manager and the Director of Information Security Practices at ISACA, which is a global association of information security, assurance and IT governance professionals located in Rolling Meadows, Illinois.

Allen C. Johnston (ajohnston@uab.edu) is an assistant professor of Information Systems at the University of Alabama, Birmingham, AL.