Enterprise Information Systems Security: A Conceptual Framework

Peggy E. Chaudhry[1], Sohail S. Chaudhry[1], Ronald Reese[2], and Darryl S. Jones[2]

[1] Department of Management and Operations/International Business, Villanova School of Business, Villanova University, Villanova, PA 19085 USA
{peggy.chaudhry,sohail.chaudhry}@villanova.edu
[2] Graduate Program, MBA, Villanova School of Business, Villanova University, Villanova, PA 19085 USA
{ronald.reese,djones21}@villanova.edu

Abstract. Over the past half a century, organizations have implemented information systems for managing their business processes. These information systems have now evolved into what are more commonly known as enterprise information systems. An important facet of implementing an enterprise information system in an organization is the development of security related issues within the information system for the business processes. In this paper, we review the relevant literature related to the security policies that are associated with the use of enterprise information systems within organizations. Based on this literature review, we identify four major issues which are security policy documentation, employee awareness, top management support, and access control. A conceptual framework based on these four issues is then presented within the context of corporate governance for the security of the enterprise information systems. We conclude our work with the future direction for this research.

Keywords: Enterprise information systems, security, conceptual model.

1 Introduction

Enterprise Information Systems (EIS) are companywide Information Technology (IT) systems that companies use to combine multiple business functions information into one data warehouse. They "enable a company to integrate the data used throughout its entire organization [1]" Enterprise information systems can include data from the various functions of an organization such as Finance (Accounts Receivable and Payable, General Ledger, Profitability Analysis, and the like.); Human Resources (Payroll, Personnel Planning, Travel Expenses, etc.); Operations and Logistics (Inventory, Purchasing, Shipping, etc.); and Sales and Marketing (Order Management, Pricing, Sales Management, etc.) [1]. The plethora of information technologies developed and improved over the last few decades has made business decisions easier for managers who now have all of the relevant information available from one access point without the fear of missing or overlapping information.

C. Møller and S. Chaudhry (Eds.): CONFENIS 2011, LNBIP 105, pp. 118–128, 2012.

A problem that results from this convenience is that all company information is now available in one location. This centrality makes a company's intellectual property, one of its core competitive advantages, more vulnerable. Security breaches (malicious or unintentional) can result in continuity disruption, poor reliability of information, lowered effectiveness and efficiency of processes, and can even have legal implications. The current events of *external* information security problems related to information access, such as the hacker who obtained the personal information of 77 million consumers at Sony's PlayStation Network is testimony to the problems that companies will continue to face with security breaches [2]. Likewise, the malware files attached to the NASDAQ's Directors Desk is clearly another recent example of outside hackers creating security violations [3]. However, in this paper, we are not addressing so-called "Hack attacks" but will be evaluating the risk of *internal* information security dilemmas, such as employees of the firm either intentionally or unintentionally compromising the data stored.

Overall, firms must safeguard their employee access to the "keys to the kingdom" (e.g., accounts and passwords) that protect an array of information ranging from credit card data, human resource personnel data, internal financial reports and research and development plans [4]. For example, in 2010, an employee of the General Services Administration of the U.S. government unintentionally compromised the social security numbers of its 12,000 staff members to a private email address that made the government agency provide identify theft coverage and credit monitoring to its employees [5].

More research on this topic is important because of the paradigm shift that we are currently facing. Until recently, most of the concern regarding security in enterprise information systems was more of a technical nature (e.g., viruses, worms, Trojans, etc.), however, more research is finding that human interaction with the systems is the real cause of most breaches [6], [7], and [8]. In fact, Sachlar Paulus, Senior Vice-President of Product and Security Governance of SAP (a global EIS provider) has stated that "The weakest link is still people … the biggest problems occur wherever technology comes into contact with people who need to administer, manage, or even use IT security functionality [9]."

The purpose of this paper is three-fold. First, we will briefly review the past work that has been done regarding security in Enterprise Information Systems and provide a succinct literature review. Next, we present a new conceptual framework that businesses can use to properly secure their data through Enterprise Information Systems. Finally, the paper concludes with a brief synopsis of plans for future research.

2 Literature Review

Up until the last few years, most of the research done on corporate dealings with security in EIS focused mainly on the technical aspect of IT such as firewalls and anti-virus software which rely more on technology than the employees using the systems [10]. In fact, as recent as 2005, Siponen [10] believed "the importance of the socio-organizational nature of (E)IS is not recognized seriously enough by traditional Information Systems Security methods." Researchers are now starting to realize that the human interaction with the EIS of the firm is just as important, if not more, than

the technical -and that information security cannot be achieved solely through these technological tools [11].

The threat of external hackers and malicious attackers of information systems are still a major issue for information security and widely reported in the current events and highlighted in practicing managers' publications, for example, see [12]. However, many researchers now believe the biggest threat to information security remains *internal* [6], [13], and [14]. Swartz [15] outlined several cases in which employees stole data while still working for their company, yet the majority of employee security breaches occur accidently or unintentionally [7] and [8]. In April 2011, Cyber-Ark® Software [4], substantiated this concern with the results of its "Snooping Survey" with respondents from Europe, the Middle East, Africa (EMEA), and the United States, with the upper echelon of managers of several companies as illustrated in Table 1.

Table 1. Have you accessed any cases on insider sabotage or IT security fraud conducted at your workplace?

	EMEA	%	US	%	C-Level	%
Yes	121	21%	137	16%	11	16%
No	303	54%	452	53%	44	63%
Don't Know	139	25%	269	31%	15	21%
Grand Total	563	100%	858	100%	70	100%

Source: Cyber-Ark Snooping Survey, April 11, 2011

This recent survey of 1,400 IT staff and C-level professionals (i.e., the CEO, CFO, COO) in both the EMEA and U.S. reveals a significant amount of these firms are aware of security breaches, or more alarmingly "don't know" if a problem exists [4]. There are currently many theories on the best way to combat these issues. These range from the importance of cultivating an information security policy to significance of employee training and awareness. Overall, just a few researchers have developed frameworks in order to help companies remain as secure as possible [14], [16], and [17].

2.1 Information Security Policy

An information security policy is the set of rules, standards, practices, and procedures that the company employs to maintain a secure IT system. This policy can contain items such as when and how an employee should access secure information and how often their passwords should be changed. It has been said that the "credibility of the entire information security program of an organization depends upon a well-drafted information security policy [18]." Also, many experts now think that the development of an information security policy is one of the most practical ways to preserve protected systems [17] and [19]. Knapp et al. [17] believe that "the development of an information security policy is the first step toward preparing an organization against attacks from internal and external sources." Sengupta et al. [20] affirms that ineffective implementation of security policy leads to weaknesses in enterprise information systems security.

One important factor that most researchers agree must be adhered to in policy development is the support of top level management [21] and [22]. The best way to get employees to comply with information security policies is to engrain the policy into the organizational culture of the company. The goal is to have employees follow and safeguard the policy as a second nature, not because the workers are being policed or audited [13]. Knapp et al. [17] actually developed an information security policy process that companies can use to develop and analyze their current programs. While security policies, procedures, and controls are the most implemented security measures, Hagen et al. [23] found through a survey of Norwegian organizations that they are not the most effective in information security.

2.2 Employee Awareness

"Creation and maintenance of security awareness include both individual and collective activities, i.e. education and awareness-raising initiatives, e.g. emails, pamphlets, mouse pads, formal presentations, and discussion groups" [23]. Many researchers now believe that employee awareness is one of the best ways to protect a company's data [16] and [24]. In fact, empirical research found that awareness creation is the most effective information security measure [23]. "Information security training and management support are possibly the most important components of an effective information security program. Training can increase security awareness, understanding, and thus, participation [25]." Systems are better protected by employees that have an enhanced understanding of the possible consequences of security breaches and are aware of ways to combat these breaches.
In addition, the extent to which employees' perceive that compliance with existing security policies are mandatory, is directly related to employees' motivation to take security precautions [6].

As illustrated in the recent Nasdaq and Sony PlayStation network cases, the increased security benefits are not only important to the sponsoring company, but its supplier and customer businesses as well [2] and [3]. Pollitt [26] actually reported a case in which a UK communications company offered free security training to customers to give them an understanding of the true risks of information security. Similar to the development and implementation of security policies, it is imperative for employee awareness to actually be an effective tool in combating poor security and top level management support is essential.

2.3 Access Control

Another commonly covered method to maintain information security is to limit employee access to certain information by roles. Access control is defined as the process a company takes to limit the access an employee has to various functions of the business; particularly functions not relevant to their position or containing more information than they should have access to [27]. She and Thuraisingham [27] stated

that many companies now use Role Based Access Control (RBAC), which is a way to limit employee access by permissions, roles, users, and constraints. In the 2011 Cyber-Ark survey, an alarming 30% of their respondents identified as IT and C-professionals (n=514 managers from the U.S. and EMEA) admitted to accessing information from a system that was *not relevant to their role* in the firm [4].

D'Aubeterre et al. [16] developed a framework to generate higher security awareness in which RBAC is an integral function. By breaking employees into roles and profiles, it is easier to determine what employee has access to which information. For example, an Accounts Payable employee should only have access to processing invoices [28]. "Monitoring user access to mission-critical information and detecting unauthorized access to high-risk data are critical steps all companies should take to better protect their sensitive information [15]." In addition, because of organizational changes or modifications of security policy, access rules have to be frequently updated. This process needs to be controlled in an efficient, adaptable and secure manner [29].

2.4 Top Level Management Support

Michael Maccoby's book, "*The Leaders We Need: And What Makes Us Follow,"* further supports the old adage of "leading by example" that is increasingly important in today's environment and he states that, "the threats and opportunities facing us have never been greater. Rapid globalization and new technologies are transforming the economy and the way we work [30]." Although Maccoby's work is not directed to IT security leadership, it is apparent that employees must perceive that top level management believes that information system security is important to the success of the company and it is engrained into the corporate culture. The overarching objective of information security management is to convert the organization's security policy into a set of requirements that can be communicated to the organization, measured, and imposed [31]. Basically, the better the top management support of information security, the greater the preventative efforts a firm (and its employees) will make [14]. Overall, top management support is essential to security governance success [32].

2.5 Corporate Governance

The research of Weill and Ross [33] on IT governance in 300 companies found that "IT governance is a mystery to key decision-makers at most companies" and that only about one-third of the managers' surveyed understood how IT is governed at his or her company (p. 26). Engulfing all of these methods for security protection is the idea of corporate governance. "Corporate governance refers to organization controls such as reporting structure, authority, ownership, oversight, and policy enforcement [32]." For information security, this is the way top level management and the board decide to run the IT department, and in turn, information system security. This is where the

true decisions on how to attack a possible weakness are made. These managerial decisions include items such as how to implement a security policy and where and how employee awareness trainings will be held. Solms [34] posits that "Information Security Governance is now accepted as an integral part of good IT and Corporate Governance (Information Security Governance)." Khoo et al. [35] stated that information security governance is a subset of corporate governance that relates to the security of information systems, and because the board of directors is ultimately in charge of corporate governance information security must start at the top [21]. To facilitate management in the governance of information security, Da Veiga and Eloff [32] developed a more comprehensive approach that combined key items from a few of the best current corporate governance frameworks.

3 Conceptual Framework

We have developed a conceptual model in Figure 1 for EIS security that encompasses the major themes found in our literature review. In its simplest form, we draw the analogy that the company's EIS security is the roof that protects four main pillars: security policy, security awareness, access control, and top level management support. The basic solid foundation of this 'house' is the company's corporate governance. As noted by Weill and Ross [33], the best performing firms in their study carefully planned their usage of IT. They further assert that, "60% to 80% of seniors executives in those companies have a clear understanding of and can describe their IT governance" (p. 26). The decisions that the leaders of the company make are the base of the entire system and will dictate the stability of it. Resting on the foundation, are the walls/pillars that support the roof. These four pillars are the processes that management and the board of directors can choose to implement to make the system as secure as possible. Having all four pillars is the best way to make the enterprise information system secure, however removing any one of these columns can truly diminish the stability/security of the entire system. Below is a pictorial representation of the model.

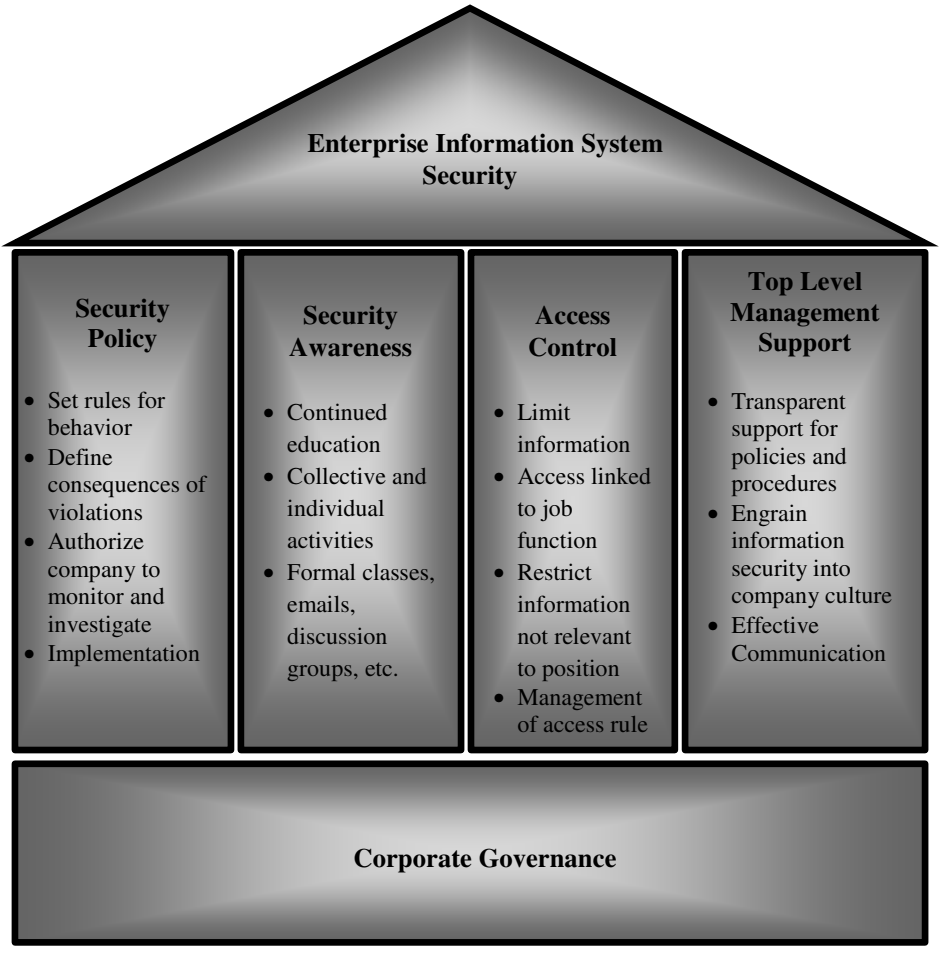

Fig. 1. Conceptual Model for Enterprise Information System Security

A summary of the research assertions in previous studies that led us to conceptualize the model in Figure 1 is provided below in Table 2.

Table 2. Constructs, Research Assertions, and Relevant Research Papers

Construct	Research Assertions	Relevant Research Papers
Security Policy	• An essential part of information security is the information security policy. • Senior level managers must plan policies in a broad and measurable way.	[13]: Vroom et al. (2004) [17]: Knapp et al. (2009) [18]: Kadam (2007) [19]: Myyry et al. (2009) [20]: Sengupta et al. (2011) [21]: von Solms and von Solms (2006) [22]: Doughty (2003) [23]: Hagen et al. (2008)
Security Awareness	• Employee awareness creation is the most effective measure for IS, but, it may be the least implemented. • Internal employees may be the biggest threat to data security. • IS training and management support are possibly the most important components of IS program. • Education is a powerful tool to ensure employees internalize IS policies. • Employees can underestimate the probability of security breaches. • Human error is important because employees may not even know they are exposing the company to information risks. • The biggest threat to intellectual property is internal, that may be either malicious or negligent employees. • Firms can give security training to their customers to educate them on the risks also.	[6]: Boss et al. (2009) [7]: Keller et al. (2005) [8]: Sumner (2009) [11]: Herath and Rao (2009) [13]: Vroom and von Solms (2004) [14]: Kankanhalli et al. (2003) [15]: Swartz (2007) [16]: D'Aubeterre et al. (2008) [19]: Myyry et al. (2009) [22]: Doughty (2003) [23]: Hagen et al. (2008) [24]: Chang and Yeh (2006) [25]: Ma et al. (2009) [26]: Pollitt (2005) [32]: Da Veiga and Eloff (2007)
Access Control	• Systems break employers into roles (essentially job titles), then into profiles (individuals in those roles), to determine who has access to what information, such as A/P employees access to processing invoices only. • Firms must develop a framework to analyze secure business processes that includes authorization and RBAC. • Companies need to monitor user access to critical information and effectively detect unauthorized access to high-risk data.	[15]: Swartz (2007) [16]: D'Aubeterre et al. (2008) [27]: She and Thuraisingham (2007) [28]: Allen (2008) [29]: Rinderle – Ma et al. (2009)
Top-Level Management Support	• Good information security governance is essential to combat human interaction risks. • The greater the top management support of IS; the greater the preventative efforts of the firm. • Information security must start at the upper echelon of the firm—the board of directors. • Top management must engrain the IS policy into the culture of the firm.	[13]: Vroom and von Solms (2004) [14]: Kankanhalli et al. (2003) [21]: von Solms and von Solms (2006) [25]: Ma et al. (2009) [32]: Da Veiga and Eloff (2007) [31]: Tracey (2007) [33]: Weill and Ross (2005) [35]: Khoo et al. (2007)

4 Conclusions and Future Research

The research in this paper has focused on how and what organizations execute to disseminate information related to security issues that evolve around the business processes with the enterprise information systems. By analyzing the relevant literature, we identified four major themes that impact the security issues within organizations. These four factors are identified as security policy documentation, access control, employee awareness, and top level management support. Based on these four factors, a conceptual framework ingrained with the relevant literature was presented within the context of corporate governance for enterprise information systems.

It is the expectations of this research that the conceptual framework developed will assist businesses protect Enterprise Information System data that could potentially be breached through socio-organizational problems. To test the framework, two future phases of this research are planned. The next phase will consist of multiple in-depth interviews with IT officers using a cross-section of companies. The companies will be of different sizes and industry sectors to get a fully holistic view of actual practices in place. Finally, with the combination of the literature review conducted for this paper, the framework presented, and the information from the interviews, a survey instrument will be developed and distributed to a larger population of IT officers to further study the various issues that have been exposed in this research within the context of enterprise information systems security.

References

1. Davenport, T.: Putting the Enterprise into the Enterprise System. Harvard Business Review 76(4), 121–131 (1998)
2. Sherr, I.: Sony Faces Lawsuit Over PlayStation Network Breach (April 28, 2011), http://online.wsj.com/article/BT-CO-20110428-720452.html (accessed on April 30, 2011)
3. Barret, D.: NASDAQ Acknowledges Security Breach (February 6, 2011), http://online.wsj.com/article/SB10001424052748704843304576126370179332758.html (accessed on April 30, 2011)
4. Cyber-Ark Snooping Survey (April 2011), http://www.cyber-ark.com/downloads/pdf/2011-Snooping-Survey-data.pdf (accessed on April 30, 2011)
5. Kalish, B.: Security Breach of Employee Data at GSA (November 8, 2011), http://techinsider.nextgov.com/2010/11/work_at_gsa_your_social_has_been_e-mailed.php (accessed on April 30, 2011)
6. Boss, S., Kirsch, L., Angermeier, I., Shingler, R., Boss, R.: If Someone is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security. European Journal of Information Systems 18(2), 151–164 (2009)
7. Keller, S., Powell, A., Horstmann, B., Predmore, C., Crawford, C.: Information Security Threats and Practices in Small Businesses. Information Systems Management 22(2), 7–19 (2005)

8. Sumner, M.: Information Security Threats: A Comparative Analysis of Impact, Probability, and Preparedness. Information Systems Management 26(1), 2–12 (2009)
9. Walsh, K.: The ERP Security Challenge (January 8, 2008), http://www.cio.com/article/216940/The_ERP_Security_Challenge (accessed on April 30, 2011)
10. Siponen, M.T.: An Analysis of the Traditional IS Security Approaches: Implications for Research and Practice. European Journal of Information Systems 14(3), 303–315 (2005)
11. Herath, T., Rao, H.R.: Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. European Journal of Information Systems 18(2), 106–125 (2009)
12. McNulty, E.: Boss, I Think Someone Stole Our Data. Harvard Business Review, 37–50 (September 2007)
13. Vroom, C., von Solms, R.: Towards Information Security Behavioural Compliance. Computers & Security 23(3), 191–198 (2004)
14. Kankanhalli, A., Teo, H.H., Tan, B.C.Y., Wei, K.K.: An Integrative Study of Information Systems Security Effectiveness. International Journal of Information Management 23(2), 139–154 (2003)
15. Swartz, N.: Protecting Information from Insiders. Information Management Journal 41(3), 20–24 (2007)
16. D'aubeterre, F., Singh, R., Iyer, L.: Secure Activity Resource Coordination: Empirical Evidence of Enhanced Security Awareness in Designing Secure Business Processes. European Journal of Information Systems 17(5), 528–542 (2008)
17. Knapp, K., Morris, R., Marshall, T., Byrd, T.: Information Security Policy: An Organizational-Level Process Model. Computers & Security 28(7), 493–508 (2009)
18. Kadam, A.W.: Information Security Policy Development and Implementation. Information Systems Security 16(5), 246–256 (2007)
19. Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., Vance, A.: What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study. European Journal of Information Systems 18(2), 126–139 (2009)
20. Sengupta, A., Mazumdar, C., Bagchi, A.: A Formal Methodology for Detecting Managerial Vulnerabilities and Threats in an Enterprise Information System. J. Netw. Syst. Manage. 19, 319–342 (2011)
21. von Solms, R., von Solms, S.H.B.: Information Security Governance: A Model Based on the Direct-Control Cycle. Computers & Security 25(6), 408–412 (2006)
22. Doughty, K.: Implementing Enterprise Security: A Case Study. Computers & Security 22(2), 99–114 (2003)
23. Hagen, J.M., Albrechtsen, E., Hovden, J.: Implementation and Effectiveness of Organizational Information Security Measures. Information Management & Computer Security 16(4), 377–397 (2008)
24. Chang, A.J.T., Yeh, Q.J.: On Security Preparations Against Possible IS Threats Across Industries. Information Management & Computer Security 14(4), 343–360 (2006)
25. Ma, Q., Schmidt, M., Pearson, J.: An Integrated Framework for Information Security Management. Review of Business 30(1), 58–69 (2009)
26. Pollitt, D.: Energis Trains Employees and Customers in IT Security. Human Resource Management International Digest 13(2), 25–28 (2005)
27. She, W., Thuraisingham, B.: Security for Enterprise Resource Planning Systems. Information Systems Security 16, 152–163 (2007)
28. Allen, V.: ERP Security Tools. The Internal Auditor 65(1), 25–27 (2008)

29. Rinderle Ma, S., Reichert, M.: Comprehensive life cycle support for access rules in information systems: the CEOSIS project. Enterprise Information Systems 3(3), 219–251 (2009)
30. Maccoby, M.: The Leaders We Need: And What Makes Us Follow. Harvard Business School Press, Boston (2007)
31. Tracey, R.P.: IT Security Management and Business Process Automation: Challenges, Approaches, and Rewards. Information Systems Security 16, 114–122 (2007)
32. Da Veiga, A., Eloff, J.: An Information Security Governance Framework. Information Systems Management 24(4), 361–372 (2007)
33. Weill, P., Ross, J.: A Matrixed Approach to Designing IT Governance. Sloan Management Review 46(2), 26–34 (2005)
34. von Solms, S.H.B.: Information Security Governance: Compliance management vs. operational management. Computers & Security 24, 443–447 (2005)
35. Khoo, B., Harris, P., Hartman, S.: Information Security Governance of Enterprise Information Systems: An Approach to Legislative Compliant. International Journal of Management and Information Systems 14(3), 49–55 (2010)