HAL
archives-ouvertes.fr

Enterprise Information Systems Security: A Case Study in the Banking Sector

Peggy Chaudhry, Sohail Chaudhry, Kevin Clark, Darryl Jones

To cite this version:

Peggy Chaudhry, Sohail Chaudhry, Kevin Clark, Darryl Jones. Enterprise Information Systems Security: A Case Study in the Banking Sector. Geert Poels. 6th Conference on Research and Practical Issues in Enterprise Information Systems (CONFENIS), Sep 2012, Ghent, Belgium. Springer, Lecture Notes in Business Information Processing, LNBIP-139, pp.206-214, 2013, Enterprise Information Systems of the Future. <10.1007/978-3-642-36611-6_18>. <hal-01484681>

HAL Id: hal-01484681

https://hal.inria.fr/hal-01484681

Submitted on 7 Mar 2017

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons Attribution| 4.0 International License

Enterprise Information Systems Security: A Case Study in the Banking Sector

Peggy E. Chaudhry[1], Sohail S. Chaudhry[1], Kevin D. Clark[1], 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, kevin.d.clark}@villanova.edu
[2] MBA Program,Villanova School of Business, Villanova University, Villanova, PA 19085
{djones21}@villanova.edu

Abstract. One important module of Enterprise Information System (EIS) is the development and implementation of the security component of EIS. Furthermore, this EIS Security structure needs to be monitored through the corporate governance of the firm. Based on a literature review and our previous work, we identified four key pillars of a model for EIS Security. These pillars are Security Policy (e.g., set rules for employee behavior), Security Awareness (e.g., continued education of employees), Access Control (e.g., access linked to employee job function), and Top Level Management Support (e.g., engrain information security into the company's culture). We explore the relevance of this model using a case study approach by way of interviewing top-level information systems mangers in the banking sector. We validate the model through using key informant in-depth interviews and qualitative research methods.

Keywords: Enterprise information systems, security, conceptual model, banking sector, case study.

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]." 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. 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]. 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) [3]. 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 [4], [5], and [6]. 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 [7].”

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. In fact, as recent as 2005, Siponen believed “the importance of the socio-organizational nature of (E)IS is not recognized seriously enough by traditional Information Systems Security methods” [8]. 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 [9]. Many researchers now believe the biggest threat to information security remains *internal* [4], [10], and [11]. Swartz [12] 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 [5] and [6]. 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 to help companies secure their systems [11], [13], and [14].

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. It has been said that the “credibility of the entire information security program of an organization depends upon a well-drafted information security policy [15].” Many experts now think that the development of an information security policy is one of the most practical ways to preserve protected systems [14] and [16]. Knapp et al. [14] believe that “the development of an information security policy is the first step toward preparing an organization against attacks from internal and external sources.” They actually developed an information security policy process that companies can use to develop and analyze their current programs.

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" [17]. Many researchers now believe that employee awareness is one of the best ways to protect a company's data [13] and [18]. In fact, empirical research found that awareness creation is the most effective information security measure [17]. Security training and education programs should aim to make employees recognize the legitimacy of information security policy to safeguard the firm [19].

2.3 Access Control

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 [20]. She and Thuraisingham [20] 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. Access control requirements can be driven by a need for customer, stockholder, and insurer confidence; privacy of personal information; prevention of unauthorized financial asset distribution and adherence to professional standards, among others [21]. In addition, so long as information is stored and consumed within one organization, security policy and access controls can be optimized for internal use, and access by people from outside of the company can be prevented [22]. However most enterprise information systems are connected to the internet, which can blur the boundaries of enterprise information systems, leads organizations to face new attack threats [23].

2.4 Top Level Management Support

One important factor that most researchers agree must be adhered to in policy development is the support of top level management [24] and [25]. 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 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 [26]. Basically, the better the top management support of information security, the greater the preventative efforts a firm (and its employees) will make [11]. Overall, top management support is essential to security governance success [27].

2.5 Corporate Governance

The research of Weill and Ross [28] 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. For information security, corporate governance 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. Solms [29] posits that "Information Security Governance is now accepted as an integral part of good IT and Corporate Governance (Information Security Governance)." Khoo et al. [30] 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.

2.6 Implementation

The careful selection and implementation of security policies, standards and procedures will determine if the overall security program will support the organization's mission [31]. So important is the implementation of these systems that national and international standards have been developed including ISO 27001, ISO 13569, GAISP (Generally Accepted Information Security Practices), and the Gramm-Leach Bliley (GLB) Act, among others [31]. Sengupta et al. [32] affirms that ineffective implementation of security policy leads to weaknesses in enterprise information systems security.

3 Conceptual Framework

We have developed a conceptual model in Fig. 1 for EIS security that encompasses the major themes found in our literature review. This model is a slightly revised version of the conceptual model that was developed earlier [33], [34]. 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 (TLMS). Each of these pillars has an element of implementation required for sound EIS Security. The basic solid foundation of this 'house' is the company's corporate governance. 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.

4 Information Security in the Banking Sector

MWR Labs identified three banking sector security risks facing the industry and two of these, data loss prevention and identity & access management, are closely related to our model [35].The banking sector is governed by a regulatory framework to

safeguard information. To highlight the regulatory governance of financial institutions to implement their information security, we briefly describe the role of the Federal Financial Institutions Examination Council (FFIEC) and the GLB Act.

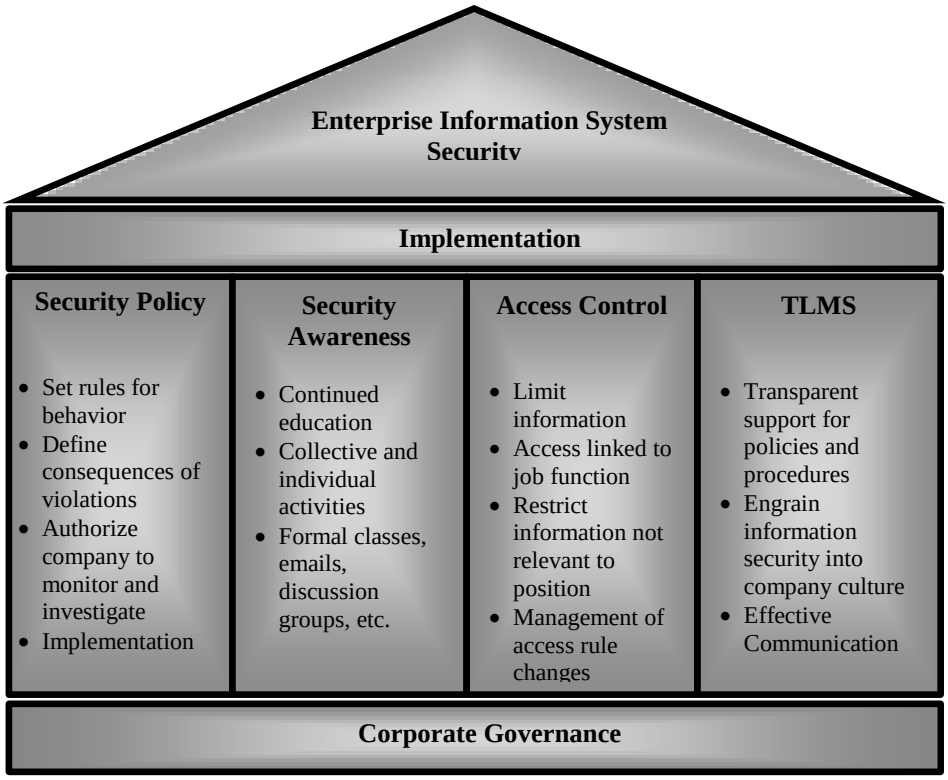

Fig. 1. Conceptual model for enterprise information system security

4.1 The Federal Financial Institutions Examination Council

The FFIEC was established in 1979 and its primary goal is "[A]a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Consumer Financial Protection Bureau" [36]. The FFIEC key areas to be addressed by financial institutions to implement information security measures [37] as 1) security process (e.g. governance issues); 2) information security risk assessment (e.g., steps in gathering information); 3) information security strategy (e.g., architecture considerations); 4) security controls implementation (e.g., access control); 5) security monitoring (e.g., network intrusion detection systems); and 6) security process monitoring and updating.

4.2 The Gramm-Leach-Bliley Act

The FDIC provides an outline of compliance issues related to the development and implementation of Information Security Program governed by the GLB Act in three key areas: involvement of the board of directors, assessment of risk, and managing and controlling risk [38]. The detailed security guidelines that banks are given to comply with the GLB Act center on [39]: 1) access controls on customer information systems; 2) access restrictions at physical locations containing customer information; 3) encryption of electronic customer information; 4) procedures to ensure that system modifications do not affect security; 5) dual control procedures, segregation of duties, and employee background checks; 6) monitoring systems to detect actual attacks on or intrusions into customer information systems; 7) response programs that specify actions to be taken when unauthorized access has occurred; and 8) protection from physical destruction or damage to customer information.

5 Qualitative Analysis of Personal Interviews with Senior Information Officers in the Banking Sector

We validate the model through using key informant in-depth interviews and qualitative research methods. We interviewed senior information officers dealing with security aspects at four banking institutions in the Philadelphia area. Next, we present the highlights of these interviews with the senior information officers based on a content analysis of the themes in the interviews.

It was quite surprising to learn from the interviews that all the four senior information officers in the banking industry agreed with the proposed conceptual security model. In addition, they all rated the four pillars of security policy, security awareness, access control, and top level management support as being extremely important for their organizations.

Under the security policy pillar, three of the four officers stated that another key element is the training of the employees. Other key elements related to security mentioned by the senior information officers include the training of top-level management and simplifying the communication of the policy to all levels of the organization.

Some of the most important aspects associated with security awareness mentioned by the senior information officers were using third-party audits to test the system and to provide training with minimal technical jargon during the training sessions.

For access control, the overarching element mentioned by all four senior information officers was the development of sophisticated measures to limit access. In addition, other key elements included avoiding carte blanche access to any employee and requiring the employees to ‘sign off’ on greater security privileges.

In regards to the most important elements of top level management support, all four senior information officers stated that top level management involvement is required due to stipulations imposed by the regulatory bodies in the banking sector. One manager stressed that overseeing the implementation of the system was a key role of top management at his financial institution.

6 Conclusions and Future Research

We identified four major themes that impact the security issues within firms. These four factors are identified as security policy documentation, access control, employee awareness, and top level management support. Based on these factors, a conceptual framework based on relevant literature was presented within the context of corporate governance for enterprise information systems. To test the framework, in-depth interviews with IT officers using a cross-section of companies in the banking sector were used to confirm the model. In the future, we will administer a survey instrument 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), accessed on April 30, 2011 at http://online.wsj.com/article/BT-CO-20110428-720452.html
3. Cyber-Ark Snooping Survey. (April 2011), accessed on April 30, 2011 http://www.cyber-ark.com/downloads/pdf/2011-Snooping-Survey-data.pdf
4. 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)
5. 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)
6. Sumner, M.: Information Security Threats: A Comparative Analysis of Impact, Probability, and Preparedness. Information Systems Management, 26(1), 2-12 (2009)
7. Walsh, K.: The ERP Security Challenge. (January 8, 2008), accessed on April 30, 2011 at http://www.cio.com/article/216940/The_ERP_Security_Challenge
8. 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)
9. 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)
10. Vroom, C., von Solms, R.: Towards Information Security Behavioural Compliance. Computers & Security, 23(3), 191-198 (2004)
11. 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)
12. Swartz, N.: Protecting Information from Insiders. Information Management Journal, 41(3), 20-24 (2007)
13. 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)
14. Knapp, K., Morris, R., Marshall, T., Byrd, T.: Information Security Policy: An Organizational-Level Process Model. Computers & Security, 28(7), 493-508 (2009)
15. Kadam, A.W.: Information Security Policy Development and Implementation. Information Systems Security, 16(5), 246-256 (2007)

16. 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)
17. Hagen, J. M., Albrechtsen, E., Hovden, J.: Implementation and Effectiveness of Organizational Information Security Measures. Information Management & Computer Security, 16(4), 377-397 (2008)
18. 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)
19. Son, J.: Out of Fear or Desire? Toward a Better Understanding of Employees' Motivation to follow IS Security Policies. Information and Management, 48, 296-302 (2011)
20. She W., Thuraisingham B.: Security for Enterprise Resource Planning Systems. Information Systems Security, 16, 152-163 (2007)
21. Sandhu, R., Cope E.J., Feinstein, H.L., Youman, C. E.: Role Based Access Control Models, IEEE, 0018-9162 (1996)
22. Sinderen, M.: Challenges and Solutions in Enterprise Computing. Enterprise Information Systems, 2:4, 341-346 (2008)
23. Wang, J.W., Gao, F. & Ip, W.H.: Measurement of Resilience and its Application to Enterprise Information Systems. Enterprise Information Systems, 4(2), 215-223 (2010)
24. 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)
25. Doughty, K.: Implementing Enterprise Security: A Case Study. Computers & Security, 22(2), 99-114 (2003)
26. Tracey, R.P: IT Security Management and Business Process Automation: Challenges, Approaches, and Rewards. Information Systems Security, 16, 114-122 (2007)
27. Da Veiga, A., Eloff, J.: An Information Security Governance Framework. Information Systems Management, 24(4), 361-372 (2007)
28. Weill, P., Ross, J.: A Matrixed Approach to Designing IT Governance. Sloan Management Review, 46(2), 26-34 (2005)
29. von Solms, S.H.B.: Information Security Governance: Compliance Management vs. Operational Management. Computers & Security, 24, 443-447 (2005)
30. 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)
31. Peltier, T.R.: Information Security Policies, Procedures, and Standards: Guidelines for Effective Security Management. Auerbach Publications, Florida (2002)
32. Sengupta, A., Mazumdar, C., Bagchi, A.: A Formal Methodology for Detecting Managerial Vulnerabilities and Threats in an Enterprise Information System. Journal of Network System Management, 19(3), 319-342 (2011)
33. Chaudhry, P., Chaudhry, S.S., Reese, R., Jones, D.S.: Enterprise Information Systems Security: A Conceptual Framework. In: Møller, C. and Chaudhry, S.S. (eds.) Re-Conceptualizing Enterprise Information Systems. LNBIP, 105, pp. 118-128 Springer (2012)
34. Chaudhry, P., Chaudhry, S.S., Reese, R.: Developing a Model for Enterprise Information Systems Security. Journal of Academic Research in Economics, 3(3), 243-254 (2011)
35. Banking Sector Security, A Report by MWR Labs, accessed on April 24 at http://labs.mwrinfosecurity.com/assets/130/mwri_annual-research-banking-review-2010-08.pdf
36. About the FFIEC, accessed on April 24, 2012 at http://www.ffiec.gov/about.htm
37. Federal Financial Institutions Examination Council, Information Security, 2006, accessed on April 24, 2012 at http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf
38. FDIC Law, Regulations, Related Acts, accessed on April 24, 2012 at http://www.fdic.gov/regulations/laws/rules/2000-8660.html
39. Langin, Daniel J.: Gramm-Leach-Bliley Security Requirements: Keeping Robbers and Regulators from the Door, accessed on April 24, 2012 at http://www.securitymanagement.com/archive/library/gramm_tech0902.pdf