ISSN: 1946-1836

Journal of Information Systems Applied Research

Volume 3, Number 16 http://jisar.org/3/16/ June 11, 2010

In this issue:

The Results of Implementing a Knowledge Management Initiative to Enhance Network Access Controls

Philip S. Kim
Walsh University
North Canton, Ohio 44720 USA

Lisa A. T. Nelson
Saint Joseph's University
Philadelphia, PA 19131 USA

Abstract: Information technology and securing information assets are growing concerns for organizations, especially those within the financial services industry. As a result, information technology (IT) audits are increasingly integral to ensuring that adequate information security controls are in place over data and information systems. Despite the growing importance of information security within the financial services industry there appears to be a lack of empirical data on the effects of conducting an IT audit and implementing recommendations as a result of audit findings. This study seeks to 1) report on a recent IT General Computer Controls Audit conducted at one financial services institution, and 2) to investigate whether the decision to strengthen the knowledge management (KM) process between the institution's Human Resources and Information Technology departments will result in fewer policy violations, thus creating a more effective information security environment. The conclusion shows that IT audits can be beneficial to organizations that rely on standard information security controls and that a knowledge management approach to implementing network access controls can significantly lower the risk of unauthorized access to corporate resources.

Keywords: IT audit, knowledge management, access controls, network access, dormant accounts

Recommended Citation: Kim and Nelson (2010). The Results of Implementing a Knowledge Management Initiative to Enhance Network Access Controls. *Journal of Information Systems Applied Research, 3* (16). http://jisar.org/3/16/. ISSN: 1946-1836. (A preliminary version appears in *The Proceedings of CONISAR 2009:* §3523. ISSN: 0000-0000.)

This issue is on the Internet at **http://jisar.org/3/16/**

The **Journal of Information Systems Applied Research** (JISAR) is a peer-reviewed academic journal published by the Education Special Interest Group (EDSIG) of the Association of Information Technology Professionals (AITP, Chicago, Illinois). • ISSN: 1946-1836. • First issue: 1 Dec 2008. • Title: Journal of Information Systems Applied Research. Variants: JISAR. • Physical format: online. • Publishing frequency: irregular; as each article is approved, it is published immediately and constitutes a complete separate issue of the current volume. • Single issue price: free. • Subscription address: subscribe@jisar.org. • Subscription price: free. • Electronic access: http://jisar.org/ • Contact person: Don Colton (editor@jisar.org)

This paper was in the 2009 cohort from which the top 45% were accepted for journal publication. Acceptance is competitive based on at least three double-blind peer reviews plus additional single-blind reviews by the board and editors to assess final manuscript quality including the importance of what was said and the clarity of presentation.

Implementing a Knowledge Management Initiative to Enhance Network Access Controls

Philip S. Kim
pxkst1@mail.rmu.edu
Walsh University
School of Business
North Canton, Ohio 44720 USA

Lisa A. T. Nelson
lnelson@sju.edu
Saint Joseph's University
Pedro Arrupe Center for Business Ethics
Philadelphia, Pennsylvania 19131, USA

Abstract

Information technology and securing information assets are growing concerns for organizations, especially those within the financial services industry. As a result, information technology (IT) audits are increasingly integral to ensuring that adequate information security controls are in place over data and information systems. Despite the growing importance of information security within the financial services industry there appears to be a lack of empirical data on the effects of conducting an IT audit and implementing recommendations as a result of audit findings. This study seeks to 1) report on a recent IT General Computer Controls Audit conducted at one financial services institution, and 2) to investigate whether the decision to strengthen the knowledge management (KM) process between the institution's Human Resources and Information Technology departments will result in fewer policy violations, thus creating a more effective information security environment. The conclusion shows that IT audits can be beneficial to organizations that rely on standard information security controls and that a knowledge management approach to implementing network access controls can significantly lower the risk of unauthorized access to corporate resources

Keywords: IT Audit, Knowledge Management, Access Controls, Network Access, Dormant Accounts.

1. INTRODUCTION

Information systems and technology have become a critical component of a company's ability to create, process, and manage data. Companies that rely on access to data must also ensure the confidentiality, integrity, and availability of such data. Information security, therefore, is a growing concern for many industries. Information security is an important topic not only within the information technology (IT) world, but also within health care, education, and corporations worldwide. It has become especially relevant within the financial services industry (Dhillon & Backhouse, 2000). A significant reason for the recent surge of interest in information security is the multitude of numerous and widely public information security breaches that have come at the expense of well known and established financial service providers, such as VISA, MasterCard, and American Express, and national retailers, such as T.J. Maxx. The public is much more aware of information security threats and breaches than ever before (Priggouris & Hadjiefthymiades, 2006). As corporations continue to grow increasingly reliant on information, the demand for information availability and reliability also brings the need for access controls to the forefront.

2. INFORMATION TECHNOLOGY AUDIT

According to the Information Systems Audit and Control Association (ISACA, 2006) the role of the IT auditor is to provide an independent assessment of the design of technology controls, determine the operational effectiveness of those controls, identify control gaps or weaknesses, and recommend solutions to address those weaknesses. Organizations rely on chief technology officers (CTOs) and IT managers to design, analyze, and implement the technologies in place. The IT audit function brings added benefit by assessing the adequacy of the controls within the data processing environment independent of the potential bias or perspective that may be held by the personnel responsible for managing the systems. An effective IT audit will provide an organization with the opportunity to guard against the potential misuse of systems due to inadequate or misplaced control gaps.

This paper describes the study of a recent information technology audit conducted by one of the authors at a financial institution located in the northeastern United States. This study itself seeks to 1) report on a recent IT General Computer Controls Audit conducted at one financial services institution, and 2) to investigate whether the decision to strengthen the knowledge management (KM) process between the institution’s Human Resources and Information Technology departments will result in fewer policy violations, thus creating a more effective information security environment. The paper concludes with the results of management's efforts to implement a knowledge management initiative to remediate the audit gaps, a discussion of the limitations of the study, and implications for potential future research.

3. ACCESS CONTROLS AND DATA INTEGRITY

In light of increasing information security breaches, fraudulent activity, and escalating security risk, an organization's ability to implement adequate access controls is of paramount importance. The challenge of managing access controls is to find the balance between providing adequate protection of information assets while still allowing enough access for workers to effectively conduct their job duties. Access controls must facilitate easy access for authorized users while, in a flexible manner, stringently exclude unauthorized users; i.e., they should not constrain creativity and collaboration (Kossek et al., 1994). Users must feel that they have access to the proper information to complete their given duties, and yet must have confidence that the confidentiality and integrity of data is maintained.

What is the consequence of not having appropriate access controls? Confidentiality and accountability may suffer within the organization. People may choose to disregard rules regarding access if they believe there are no negative consequences proceeding from their actions. Adequate authentication mechanisms are needed for computer systems so that responsibility and accountability can be assigned to a specific user (Dobni, 2006).

Why is data integrity so important? If we understand that information or data are what companies use to make decisions that can significantly impact their businesses, relationships with customers, and future strategic plans, then accurate information is a necessity in today's world (Dhillon & Backhouse, 2000).

ISACA (2006) provides a framework called the Control Objectives for Information and Related Technology (COBIT) guidelines, to measure information security standards and adequate access controls. “Effective access security controls can provide a reasonable level of assurance against inappropriate access and unauthorized use of systems” (Ruckman, 2002, p.23). Simply put, access controls can protect information by restricting access to corporate resources based on a role-based “need-to-know and need-to-have” model.

Setting up strong authentication access controls can be difficult due to the high level of maintenance required for network administrators. Supporting end users and helping them to recover passwords and resetting user access rights will require additional resources and time. Companies are also struggling to implement solid access controls because there is a constant push towards improving efficiency, providing exceptional customer service, and improving the company's bottom line, which can often be viewed in direct opposition of enhancing information security controls. Management is eager to provide consumers with quality service often to the detriment of security standards and prudent access controls (Baggett, 2003).

4. INFORMATION SECURITY RISKS AND THREATS

Insider Threats

What or who are the primary threats to a corporation's internal network data? A recent industry survey indicates that the greatest risk of unauthorized access to networks is from inside sources (Sveen, Rich, & Jager, 2007). Security breaches vary in intent and purpose (e.g., from a curious employee utilizing network access to gain confidential company or employee information to a disgruntled employee using internal access to propagate a virus to infect a company's most valuable database). Corrupt staff or dishonest visitors can easily copy information from a financial institution's main systems to a multitude of external storage devices, such as USB flash drives, digital cameras, MP3 players, and mobile phones—all of which then become vulnerable if subsequently lost, stolen or recopied (Cox, 2002; Richardson, 2007). Insider abuse of network access can also include using corporate network resources for personal and unethical use. Survey responses in the aforementioned 2007 CSI survey showed an increase in insider abuse of network resources to 59% from 42% the previous year (Squier & Snyman, 2004). A review of who has access to the internal network environment is critical to determine how effective a financial institution is adhering to regulatory guidelines and industry best practice.

5. RESEARCH METHODOLOGY

One of the authors, a Certified Information Systems Auditor (CISA) completed an Information Technology General Computer Controls (ITGC) audit for a financial banking institution located in the Northeastern United States. The financial banking institution had scheduled an IT audit to review the organization's information technology data and settings for the months of January through November 2008. The audit was conducted over 21 consecutive days in November 2008. The authors were able to access all archived log report files and audit-related data, subject to a nondisclosure agreement.

The CISA met with the IT manager, and the IT security supervisor, and the helpdesk supervisor to discuss the scope of the audit, the current computer and networking environment. He also scheduled meetings to ensure all relevant personnel and staff were available for audit interviews. The majority of the audit meetings took place within the bank's Operations Center, which houses the bank's Data Center, and is also where the bank's Information Technology personnel are located. The bank, which comprises over 55 branches in the Northeast United States, employs over 1,000 employees.

To ensure the corporate policies and standard operating procedures documents are current, the bank reviews and presents the documents for approval by the bank's Board of Directors on an annual basis. The auditor noted that all policies and procedures reviewed during the audit were approved by the Board on various dates throughout the year.

The physical security review consisted of taking a tour through the bank's operational facilities, a walk-through of several back office and branch locations, and the main Data Center. The auditor reviewed logical security, access controls, dormant accounts, and security policy settings by observing policy settings, obtaining system reports, comparing parameter settings to the audit program, and reviewing network topology diagrams. The auditor also conducted interviews and meetings with personnel from the Information Technology and Human Resources departments.

6. FINDINGS

The following corporate policies (Table 1) were reviewed to ensure they adequately address purpose, scope, responsibilities, and enforcement as related to IT general computer controls. The auditor reviewed the board committee minutes to ensure all policies were formally presented and approved by the Board of Directors.

TABLE 1

Policy #	Computer Systems Policies & Procedures:	Board Approval:
301	Computer Software and Systems Purchases	1/13/2008
302	Personal Computer, Network Use and Security	1/13/2008
303	E-mail Communications	2/15/2008
304	Internet Access	4/7/2008
305	Website Development	4/7/2008
306	Intranet Publishing	4/7/2008
308	Technology Asset Disposal	5/5/2008
309	Information Systems Change Management	5/5/2008

The CISA observed that the bank has placed adequate physical controls over the operational facilities, back office and branch locations, and the main Data Center. The auditor visited the bank's Operations Center during the non-business hours on the weekend of November 14, 2008 to attempt to gain physical access to the building. The auditor noted that the bank's operational facilities, record retention areas, and the Data Center have all been secured with card-key access doors that remain locked 24 hours per day, seven days per week. The bank also requires all visitors to sign in and to receive a visitor's badge to noncustomer-contact areas.

Entrance to the Data Center server room requires two different card-keys due to the bank implementing two separate security zones to reduce the risk of unauthorized physical access. In addition to the locks and restricted access, the Data Center has been equipped with motion sensors and thermal monitors; these safeguards are intended to detect unauthorized access during non-business hours and to warn of the risk of fire or system malfunctions due to overheating.

The auditor reviewed the network login settings. The network authentication process requires the user to choose a unique user ID and password; the password must be made up of alphanumeric keys and one special character (e.g., # or @) and be at least eight characters in length. The number of sign-on attempts is set to three; users are indefinitely locked out upon three unsuccessful login attempts. The password history is set to "indefinite," which reduces the risk of password recycling. Password recycling should be restricted in order to encourage users to create and utilize new passwords, rather than simply going through the procedure of resetting a new password to an existing password. The auditor reviewed the user profiles of the system administrators, database administrators, and other power user profiles that have the ability to modify or delete other network user settings and read/write access to system security fields. As a part of the audit program, the auditor also reviewed all users that have remote access into the RAS server, to ensure all user profiles were current and necessary per job duties and responsibilities. The auditor reviewed the internal network activity log to view all network administrator and remote access activity during the third quarter of 2008. The auditor noted there was no unusual activity. The logical security settings in place appeared to be adequate to prevent misuse by Network Administrators.

The auditor selected four application server backup tapes from February 10, April 17, July 2, and October 20, 2008. The backup media was tested to ensure the integrity and availability of the backup tapes. The auditor was able to observe the network backup process and no exceptions were noted.

Audit Exception

An audit exception was noted regarding the existence of dormant network user accounts. The network user accounts in question were identified as dormant and not set to "disabled." The ITGC audit steps included a review of the daily internal Network Access Log (NAL) report, which provides a listing of all network users and the dates and times of their last successful login sessions. The NAL report collects data on each of the users' login sessions and lists all users that have not logged in to the network in over 14 days. If the user had not signed on in over 14 business days, then the user's network access should be "disabled." The Disabled Status allows the auditor to determine if the user’s network account is active or inactive. When the Disabled Status is set to “True,” the user’s network access is revoked indefinitely. If the Disabled Status remains “False,” then the user’s network access remains active.

If a user’s network access is revoked, then the user’s supervisor must formally request the Disabled Status to be set to “False,” thereby reinstating the user’s network access credentials. The process of changing a user’s network access rights is a manual process. The change request must begin with the completion of a Change Request Form that is signed off by the end user’s supervisor, reviewed by Human Resources and finally forwarded to Information Technology for completion. While the NAL report is automated, the actual change of the user’s access requires the Information Technology department to manually set the user’s Disabled Status to “True” or “False.”

The NAL report (Appendix A) lists *Full Name*, *Network Domain*, *User Name*, *Login Time*, and *Login Disabled Status*. For the purposes of this study the authors have removed confidential and proprietary information, such as that in the Network Domain and User Name fields, and have replaced full names with User 1, User 2, User 3, etc. The authors have added two additional fields, *Violation* and *Reason*. According to the bank’s internal corporate policy, a user profile was said to be in violation of the company policy if the user had not signed on in over 14 days and if the Login Disabled field was set to “*False*.” This meant that, even though there was a period of inactivity of over at least 14 days, the user's profile was still active and able to successfully accept a login.

The CISA noted that with the current manual process in place, there is a potential lag time of user access changes due to physical department location, distance from the main data center, and the time it takes to manually complete, review, and forward paper documents. In order to reduce the problem of false-positive exceptions, the auditor noted only those users that had not signed onto the network before October 1, 2008, thus giving a grace period of 19 days, versus the corporate policy of 14 days. The authors have noted in *bold* to identify the existence of violation.

During the ITGC Audit, the CISA discussed the potential information security risks of the existence of dormant, or stale, accounts. A brief description of dormant accounts is warranted here, as they represent a significant finding within this study. *Dormant* is defined as a state of rest or inactivity (FDIC, 2000). Dormant accounts, therefore, are network user profiles that have not been accessed within a specified period of time. They can sit unnoticed by system administrators until an attacker finds them and uses them to access unauthorized information (Cobanoglu & DeMicco, 2007). The time period of inactivity to be considered as dormant may differ from organization and industry. Network inactivity may be viewed as higher risk within military operations or healthcare versus less risk within the retail or manufacturing industry. Although time periods may differ from various companies, most network administrators do understand the benefit of establishing a time limit for account dormancy.

Dormant accounts may be present within every company. They are usually from legitimate users and former employees who have left the company, or have transferred to other departments and no longer need their original access levels. The existence of dormant accounts increases the opportunity for an ambitious attacker to access the company's internal network and have free reign without blame. The existence of dormant accounts reduces the company's ability to hold users accountable for their actions. Internal attackers will often follow the path of least resistance, and we posit that unmonitored dormant accounts are one of their easiest targets.

Upon initial inquiry of why the users had not logged in, the IT department was not aware of the specifics reasons for user inactivity. A discussion with the HR department yielded legitimate reasons for user inactivity, e.g., absence due to Family Medical Leave Act (FMLA), other extended leave, retirement, and termination (Table 2). While the reasons for user accounts becoming dormant appeared to be reasonable, the user profiles were still listed as active, which clearly posed a risk of circumvention of access controls.

TABLE 2

PRE-Knowledge Management Initiative

Dormant Accounts:		**10/19/ 2008**
User Accounts in Violation		
Reasons for Dormancy:	**No. of Users:**	**%:**
Retired	1	1.72%
Extended Leave	16	27.59%
Generic Sign-on	10	17.24%
Temporary User-IDs	2	3.45%
Transfer	1	1.72%
User Accounts NOT in Violation		
Legitimate Active Login	21	36.21%
Legitimate Disabled Login	7	12.07%
TOTALS:	**58**	**100.00%**

Upon completion of the audit, the access control exception was noted, and the auditor included a recommendation for management to consider formalizing a communication method of sharing knowledge between the Human Resources and Information Technology departments. The network access change requests should be reviewed by the HR department immediately upon receipt and a process should be in place to notify the IT department of all employment status changes as soon as practicable.

7. KNOWLEDGE MANAGEMENT

Both the human resources and IT departments of the financial banking institution in this study exhibited tacit knowledge; however, these departments did not exhibit the ability or the willingness to work together to articulate (i.e., to make explicit) and to share this knowledge. As a result, they have increased the level of information security risk to the bank. Effective knowledge management practices would eliminate the reliance on tacit knowledge, and allow different departments to work together and share knowledge more readily.

According to Tiwana (2002), one reason to conduct a knowledge audit is to strengthen a competitive weakness. Several case studies have been done in the financial services industry to illustrate that knowledge sharing and effective knowledge management are essential to enhancing competitive advantage, in part by keeping data secure (Dovey & Fenech, 2007).

How do we get there from here? To a degree, the shift from an environment reliant on tacit knowledge to one of explicit knowledge begins with adapting the organizational culture to overcome any managerial resistance to sharing information (Dovey & Fenech, 2007). Adopting a more common-goal, customer-oriented focus may assist with accomplishing this organizational cultural shift. Kossek et al. (1994) claim that attitudinal ambivalence between human resources and information technology toward knowledge systems and sharing can be resolved for the benefit of the organization; these departments can become strategic partners in achieving organizational goals (Talone et al., 2005). Changing the culture begins with engaging employees in both HR and in IT to gain their commitment to be agents of cultural change. An extensive discussion of KM-related initiatives to enact culture change are beyond the scope of this paper; however it is necessary to note the influence of culture on how an organization uses, stores, and shares knowledge.

Table 3 is similar to Table 2; however, it illustrates the profiles *after* management implemented an HR and IT Knowledge Management initiative involving a daily notification process of disabling dormant accounts and sharing employment status changes immediately within an HRM system that is housed on the network with limited access.

Finally, a chi-square analysis (Table 4) reveals a strong correlation between the implementation of knowledge management practices between HR and IT and the resulting reduction of dormant network accounts. The dependent variables are classified as "Accounts in Violation" and "Accounts Not in Violation." The independent variable is classified as "PRE-KM Initiative" and "POST-KM Initiative."

The authors reviewed a Network Access Log report dated mid-February 2009, approximately two months after management's action to integrate a Knowledge Management process between HR and IT. The benefit of the KM initiative on this organization is clear. The data analysis returns a significance/correlation level of ***.027***. This shows that, for this financial institution, a strong correlation exists between the KM initiative and the reduction of unauthorized network accounts. These results can reveal the effectiveness of this organization's collaborative approach to enhancing their security control environment by reducing the amount of dormant network accounts.

TABLE 3

POST-Knowledge Management Initiative

Dormant Accounts:		**02/15/ 2009**
User Accounts in Violation		
Reasons for Dormancy:	**No. of Users:**	**%:**
Retired	0	0.00%
Extended Leave	1	4.76%
Generic Sign-on	4	19.05%
Temporary User-Ids	0	0.00%
Transfer	0	0.00%
User Accounts NOT in Violation		
Legitimate Active Login	2	9.52%
Legitimate Disabled Login	14	66.67%
TOTALS:	**21**	**100.00%**

TABLE 4

	PRE-KM Initiative **10/19/08**	**POST-KM Initiative** **02/15/09**	**Total:**
Accts In Violation	30	5	**35**
Accts Not In Violation	28	16	**44**
Totals:	**58**	**21**	**79**

Degrees of Freedom: 1

Chi-square: 4.8687437357

*P is less than or equal to **0.027***

8. CONCLUSION

The key implication of this study is that the assignment of responsibilities for ensuring appropriate network access controls should not rest on one primary individual or department. A collaborative knowledge management approach to achieving stronger access controls has been proven to be effective. For this organization, an effective method to manage the network access controls was to ensure that the human resources and information technology departments were proactively sharing knowledge and increasing inter-departmental dependencies as a part of the hiring, termination, and user access change process. For a company to grow and to enhance their control environment a continual reassessment is also necessary; a one-time review of security and internal controls is not enough. An ideal way to continually and proactively reassess a control environment is to solicit and involve other departments' input (Bhatti, Bertino, & Ghafoor, 2007).

A teamwork approach by the human resources and information technology departments has enabled the human resources representatives and network administrators to conduct their duties more effectively. Organizations that have not considered actively involving other departments within their network access controls process should consider the results of this study when deciding whether implement a more collaborative approach to enhancing information security.

Additionally, the organization has recognized the value of conducting an IT audit over the computer and network environment. Though there are advantages to self-assessments that review in depth system implementation and analyses, the inherent drawback is the lack of objectivity and independence. The benefit of having an IT audit conducted by a Certified Information Systems Auditor is that the auditor should have expert knowledge of general computer controls, be aware of the various regulatory guidelines, and should have a strong understanding of risks and controls associated with the information systems environment. Often, an IT auditor will be responsible to report all findings and exceptions to different line of authority such as the Audit or Risk Committee, providing additional independence from undue influence from operational management.

Discussion

The majority of research and literature on information security focuses on software and automated controls; however, this study involved human intervention. Sabherwal and Becerra-Fernandez (2003) conducted a study within the National Aeronautics and Space Administration (NASA) and found that within the context of a knowledge management initiative, the employees' actions at the individual level can have a significant impact on the organization at the enterprise level. The knowledge management process not only increased information sharing among individuals, it created an environment where information was shared more effectively across departments and organization-wide. Similarly, information security is not simply a technical issue. It is a social and organizational problem because the technical systems have to be operated by and serve the needs of people. A more holistic view of information security and how it fits into the overall organizational structure is necessary. The knowledge management initiative in this study brought about a change in employees' actions, affecting not only their own departments, but creating stronger network access controls. This in turn affected the overall information security environment of the bank.

Future Study

This study was limited in time and scope to one IT general controls audit. A follow-up audit is planned for 2010 to evaluate the knowledge management initiative's effectiveness over an extended period of time; the positive correlation in the results may be attributed in part to the limited time scope of the IT audit (i.e., issues identified in the audit were corrected and not enough time lapsed for them to recur).

This study also was limited to one financial services organization and to its internal, local area network access. With the growing acceptance of wireless networks and personal computing devices to conduct business with financial services clients, additional studies of external and remote network access controls within these applications should be considered. Preventing unauthorized access to confidential data will continue to be significant concern within the financial services industry.

9. REFERENCES

Baggett, W. (2003). Creating a culture of security. *Internal Auditor*, *60*(3), 37-41.

Bhatti, R., Bertino, E., & Ghafoor, A. (2007). An integrated approach to federated identity and privilege management in open systems. *Communications of the ACM*, *50*(2), 81-87.

Cobanoglu, C. & DeMicco, F. J. (2007). To be secure or not to be: Isn't this the question? A critical look at hotel's network security. *International Journal of Hospitality & Tourism Administration*, *8*(1), 43-59.

Cox, J. (2002). Survey: Security remains job 1. *Network World* [Electronic Version]. Retrieved February 10, 2009, from http://www.networkworld.com/news/2002/0520nw500.html.

Dhillon, G. & Backhouse, J. (2000). Information system security management in the new millennium. *Communications of the ACM*, 43(7), 125-128.

Dobni, C. B. (2006). Developing an innovation orientation in financial services organizations. *Journal of Financial Services Marketing*, *11*(2), 166-179.

Dovey, K. & Fenech, B. (2007). The role of enterprise logic in the failure of organizations to learn and transform. *Management Learning*, *38*(5), 573-590.

FDIC Corporation. (2000). Proposed Security Standards for Customer Information, FIL-43-2000, July 2000.

ISACA. (2006). *IT control objectives for sarbanes-oxley* (2nd ed). Rolling Meadows, IL: ISACA.

Kossek, E. E., Young, W., Gash, D. C., & Nichol, V. (1994). Waiting for innovation in the human resources department: Godot implements a human resources information system. *Human Resource Management*, *33*(1), 135-159.

Priggouris, I. & Hadjiefthymiades, S. (2006). A distributable security management architecture for enterprise systems spanning multiple security domains. *Electron Commerce Research*, *6*(3-4), 355-388.

Richardson, R. (2007). *2007 CSI computer crime and security survey*. San Francisco, CA: Computer Security Institute. Retrieved February 15, 2009, from http://www.gocsi.com.

Ruckman, S. (2002). Helping protect computer networks from the inside. *Journal of Internet Law*, October 2002, 8-9.

Sabherwal, R. & Becerra-Fernandez, I. (2003). An empirical study of the effect of knowledge management processes at the individual, group and organizational levels. *Decision Sciences*, *34*(2), 225-260.

Squier, M. M. & Snyman, R. (2004). Knowledge management in three financial organizations: A case study. *Aslib Proceedings*, *56*(4), 234-242.

Sveen, F. O., Rich, E., & Jager, M. (2007). Overcoming organizational challenge to secure knowledge management. *Information Systems Frontiers*, *9*(5), 481-492.

Tiwana, A. (2002). *The knowledge management toolkit* (2nd ed.). Upper Saddle River, NJ: Prentice-Hall.

Tolone, W., Ahn, G. J., Pai, T., & Hong, S. P. (2005). Access control in collaborative systems. *ACM Computing Surveys, 37*(1), 29-41.

APPENDIX A

Network Access Log (NAL) Report

(*Bold denotes violation)

10/19/2008					
#:	**Name:**	**Login Date:**	**Login Disabled:**	**Violation*:**	**Reason:**
1	User 1	10/4/2008	FALSE	No	
2	User 2	10/3/2008	FALSE	No	
3	User 3	9/21/2008	FALSE	**Yes**	**Retired**
4	User 4	10/5/2008	FALSE	No	
5	User 5	10/2/2008	FALSE	No	
6	User 6	10/4/2008	FALSE	No	
7	User 7	10/3/2008	FALSE	No	
8	User 8	9/25/2008	FALSE	**Yes**	**Extended Leave**
9	User 9	9/17/2008	FALSE	**Yes**	**Extended Leave**

10	Generic User ID 1	1/13/2008	FALSE	**Yes**	**Generic Shared Sign-on**
11	User 10	10/5/2008	FALSE	No	
12	User 11	9/13/2008	FALSE	**Yes**	**Extended Leave**
13	User 12	9/10/2008	FALSE	**Yes**	**Extended Leave**
14	User 13	10/6/2008	FALSE	No	
15	User 14	10/6/2008	FALSE	No	
16	User 15	9/26/2008	FALSE	**Yes**	**Extended Leave**
17	User 16	9/28/2008	FALSE	**Yes**	**Extended Leave**
18	Temporary User ID 1	1/31/2007	FALSE	**Yes**	**Temporary User ID**
19	Generic User ID 2	3/6/2008	FALSE	**Yes**	**Generic Shared Sign-on**
20	User 17	10/3/2008	FALSE	No	
21	Generic User ID 3	8/23/2007	FALSE	**Yes**	**Generic Shared Sign-on**
22	User 18	9/26/2008	FALSE	**Yes**	**Extended Leave**
23	Generic User ID 4	7/10/2008	FALSE	**Yes**	**Generic Shared Sign-on**
24	User 19	8/17/2008	FALSE	**Yes**	**Extended Leave**
25	User 20	10/1/2008	FALSE	No	
26	User 21	10/5/2008	FALSE	No	
27	User 22	7/25/2008	FALSE	**Yes**	**Extended Leave**
28	User 23	10/6/2008	FALSE	No	
29	User 24	10/5/2008	FALSE	No	
30	User 25	10/3/2008	FALSE	No	
31	User 26	10/5/2008	FALSE	No	
32	User 27	10/5/2008	FALSE	No	
33	User 28	10/3/2008	FALSE	No	
34	User 29	10/1/2008	FALSE	No	
35	User 30	10/4/2008	FALSE	No	
36	Generic User ID	8/21/2008	FALSE	**Yes**	**Generic Shared**

	5				**Sign-on**
37	Temporary User ID 2	6/9/2007	FALSE	**Yes**	**Temporary User ID**
38	User 31	1/25/2008	FALSE	**Yes**	**Extended Leave**
39	Generic User ID 6	1/25/2008	FALSE	**Yes**	**Generic Shared Sign-on**
40	Generic User ID 7	8/22/2008	FALSE	**Yes**	**Generic Shared Sign-on**
41	Temporary User ID 3	6/20/2006	FALSE	**Yes**	**Temporary User ID**
42	User 32	7/26/2008	FALSE	**Yes**	**Transferred**
43	Generic User ID 8	2/21/2008	FALSE	**Yes**	**Generic Shared Sign-on**
44	User 33	6/4/2008	FALSE	**Yes**	**Extended Leave**
45	Generic User ID 9	6/4/2008	FALSE	**Yes**	**Generic Shared Sign-on**
46	User 34	10/5/2008	FALSE	No	
47	User 35	9/12/2008	FALSE	**Yes**	**Extended Leave**
48	User 36	9/4/2008	FALSE	**Yes**	**Extended Leave**
49	User 37	9/25/2008	FALSE	**Yes**	**Extended Leave**
50	User 38	8/3/2008	FALSE	**Yes**	**Extended Leave**
51	User 39	9/24/2008	FALSE	**Yes**	**Extended Leave**
52	User 40	10/12/2008	TRUE	No	
53	Generic User ID 10	4/10/2002	TRUE	No	
54	User 41	5/25/2008	TRUE	No	
55	User 42	8/14/2008	TRUE	No	
56	Generic User ID 11	10/10/2007	TRUE	No	
57	Generic User ID 12	6/10/2008	TRUE	No	
58	User 43	8/14/2008	TRUE	No	

(*Bold denotes violation)