Journal of International Technology and Information Management

Volume 18 | Issue 1 Article 7

2009

Business Risks: When IS Fails to Detect Circumvention Activities

Stanley X. Lewis Jr.
Troy University

J. Scott Magruder
University of Southern Mississippi

Eddy J. Burks
Troy University

Carl Smolinski
Louisiana State University- Shreveport

Business Risks: When IS Fails to Detect Circumvention Activities

Stanley X. Lewis, Jr.
Troy University
USA

J. Scott Magruder
University of Southern Mississippi
USA

Eddy J. Burks
Troy University
USA

Carl Smolinski
Louisiana State University-Shreveport
USA

ABSTRACT

A business must recognize and address various risk factors when establishing and maintaining its information system. The overall risk to management is that the control environment does not protect proprietary business data and the financial reporting system that produces financial statements and other information used by investors, creditors and regulatory agencies. These risks require that management implement efforts to ensure the integrity and effectiveness of control procedures over business activities while being aware of additional system issues such as failing to adequately consider other risks which are more business-oriented including the risk of failing to prevent or detect fraudulent or illegal activities. Worldwide in 2008 the value of economic data stolen was estimated to be a trillion dollars. After the public outcry from the business failures such as Enron there were efforts by the U.S. government, business community and the accounting profession to strengthen business control environments to better address such risk factors and thereby improving the quality of financial data. One result of these efforts has been that businesses are guided by the features of the Sarbanes-Oxley Act (2002) and efforts by COSO (2007) which indirectly allude to but do not specifically address these risk factors in a technology-based business environment. Currently almost all records maintained by a business organization are now in an electronic format with over two-thirds never converted to hard copy. The integral nature of a networked system necessitates having adequate control aspects that ensure the confidentiality of business proprietary data and to ensure this data is not stolen or misused. One aspect of this issue is that of insider hacking to transfer or misuse proprietary business data. This issue and recommendations for management and their auditors are reported in this research.

INTRODUCTION

In 2008 an estimated one trillion dollars was lost due to the theft of proprietary business data worldwide (McMillan, 2009). Reacting to this potential loss (or fraud) a business must address

different risk considerations when it designs, implements and/or attempts to improve its control environment. Two different internal views of risk must be utilized by the business as it reacts to the potential for loss due to theft of economic data or business proprietary data. One view is that of business risk or the failure to maintain adequate managerial oversight and control over the day-to-day operations designed to assist the business in achieving stated goals and objectives (Internal Risk Level One). A second view is the operational risk or the failure to establish procedures that ensure the day-to-day operations work effectively and efficiently (Internal Risk Level Two). Operational risk is more in-depth (detailed) and includes the possible weaknesses and/or failures of the information system department tasked to provide a secure system for the business. A secure system would include specific procedures which will either be system-driven tools and techniques or implemented manually by employees to prevent and/or detect the theft of proprietary data.

Annually both internal business and operational views of risks are reviewed, utilized and evaluated by the business' external auditors (EA) during the planning and completion of the annual audit of the financial statements so there is external consideration of the success and failure of the business in controlling these risk factors. This external consideration is necessary since the results of the business' financial reporting system and the related audit report are used by creditors, current and potential investors and regulatory agencies. However, the EA's (and the expanded accounting profession) view of risk is often overlooked by the information system (IS) staff as they focus on the internal detailed needs of the business system. One result of overlooking the EA evaluation of the business' risk exposure by the IS staff is a disconnection between IS operation and external expectation. This disconnection should be kept to a minimum or eliminated if the business is to be successful in managing its risk factors.

Risk Factors

A useful starting point is to understand the end result a business desires from its control environment if it is to effectively implement controls that eliminate or minimize the theft of economic data. Thus, we begin with the EA that provides direct assurance to creditors, investors and regulatory agencies that the results, financial statements, of the financial reporting system of the business consists of fairly presented financial information and indirect assurance that the client has an effective, well-managed system that reduces the likelihood of the theft of proprietary data and/or manipulation of business information. The EA serves as the last check of reliability before business data is made available to the public, i.e., creditors, investors, regulators, etc., and serves to establish credibility about the fairness of presentation of the business data as presented in the financial statements.

The EA focuses on the issue of risk from two principle perspectives: 1) internal to the client organization and 2) external from the view of the auditor. These perspectives are attempts to simplify the evaluation of risk using descriptive methods and are designed to include updating risk perspectives for current changes in the global business environment including the increasing issue of theft of economic data. Surveys have described the fact that more than 90% of all business records are currently maintained in some type of electronic format as well as estimating that 70% or more of these records are not ever converted to hard (printed) copy; thus, traditional descriptive efforts to evaluate (and thus manage) risk are showing signs of aging (Montague, 2007). Well-intended management efforts to demonstrate compliance with guidelines

established by Sarbanes-Oxley and COSO with controls including those addressing economic data theft as well as general business risk might still be unacceptable when an IS operations weakness could be exploited by an employee to circumvent IS procedures over the financial reporting system which allows management to investigate.

External Risk

The EA or certified public accountants (CPAs) engaged to audit financial statements prepared by a client's financial reporting systems are required to assess the risk of material misstatement (RMM) describing a client's internal risk (both inherent risk and control risk – discussed below). However, additional risk categories must be considered in order for the EA to develop a complete understanding and consideration of the entire spectrum of risk related to a specific business audit client - detection risk and audit risk.

Detection Risk (DR). The failure by the EA to detect and assess correctly the internal (to the corporation) risk factors and thereby not correctly assessing risk and thus being associated with misleading financial statements and an incorrect audit report with resulting issues raised by all external user groups. An EA will attempt to manage his/her risk by considering two types of risk: (1) tests of details risk (TD) or the risk that audit procedures did not detect material weaknesses in the client's internal control system that underlies its financial reporting system, and (2) substantive analytical procedures risk (AP) or the risk that audit procedures applied beyond those "test of details" procedures did not detect material weaknesses in the financial statements produced by the client's financial reporting system.

Audit Risk (AR). The cumulative risk that an EA is associated with materially misstated financial statements by incorrectly assessing the various components of the EA's risk during an audit and is a cumulative perspective of all risk factors (inherent, control and detection). The AICPA describes a general model for understanding the general relationship of audit risk and the other risk components described above and thereby control overall risk of releasing a report associated with a set of financial statements by the use of numerical calculations

- AR = RMM x DR
- RMM = Inherent Risk (IR) x Control Risk (CR)
- DR = Detection Risk

The external auditor can manage (and thus control) DR during audit planning and the subsequent application of audit procedures (TD and AP) and are found in common audit practice guides used within the profession. (AICPA, 2007; AICPA, Internal Control, 2005) The rationale is simple, the auditors wish to reduce or restrict their legal exposure or liability to investors, employees and other stakeholder groups. Evidence gathered by CPAs during the conduct of an audit of financial statements prepared (and thus subsequently published or distributed) in a client's financial reporting system should also be examined from two other perspectives: (1) the detection of fraud, and (2) the impact of technology on the financial reporting system and the related internal control system. In essence the external auditor will attempt to control his/her risk of being associated with a client (business) that also has risks. The EA and the business attempts

to reduce or eliminate the potential for litigation claims that investors' losses are the result of mismanagement.

Internal Risk

The risk that is internal to a corporation and thus the primary focus of the IS staff is the risk that efforts by corporate management will not result in an efficient and effective system of internal control and that internal monitoring will not reveal or detect control weaknesses and problems in a timely manner to assist the board of directors and management in achieving its financial reporting objective. Risk management is how these efforts are commonly referred to and it as an area of consideration by corporate management and has evolved through the years as the failures of businesses have been made public and resulted in regulatory action and often the passage of statutory laws designed to improve the financial reporting process vital to investors, employees and other stakeholder groups (COSO, 2004).

The National Commission on Fraudulent Financial Reporting established what became known as the Treadway Commission to address several issues including the IR issue as the accounting professional and the greater business community has undertaken efforts to address flaws and weaknesses in the financial reporting efforts by regulated public businesses. In 1992 the Treadway Commission released Internal Control—Integrated Framework as a guide to the business community and thus, the accounting profession, as an effort to provide a structure for corporations to use in efforts to improve the existing financial reporting systems used. This guide defined internal control as "a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives" in three categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations.

The Commission stated success or failure of the internal control process is based upon a judgment of its effectiveness by the company's board of directors and management efforts in achieving reasonable assurance that:

- They understand the extent to which the entity's operations objectives are being achieved.
- Reliably published financial statements are being prepared.
- They are in compliance with applicable laws and regulations (AICPA , 2005).

A subsequent or follow up to the 1992 Treadway Commission effort was undertaken and completed by the Committee of Sponsoring Organizations (COSO), subunit of the Treadway Commission, in 2001 led to the issuance an updated guide or framework known as Enterprise Risk Management Integrated Framework (COSO, 2004) incorporating evolving issues since 1992 and several highly public financial reporting and business failures. Congressional action resulted in the enactment of the Sarbanes-Oxley Act of 2002 (COSO, 2004).

The updated framework was completed and circulated in 2004 and provided an updated structure for corporate management and board of directors in their efforts to evaluate and improve what was then being labeled Enterprise Risk Management (ERM) after a series of high-profile

business failures (and the corresponding audit failures by the accounting profession) that had led to investors, employees and other stakeholders suffering significant losses. The goal of COSO was to provide an improved and more complete framework that incorporated changes in how business was conducted and was one of several attempts by the accounting profession to respond to the perceived failures of public accounting firms in the series of business failures and the enacted Sarbanes-Oxley Act of 2002. In the 2004 guide Enterprise Risk Management (ERM) was defined as follows:

> Enterprise risk management is a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and management risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives (COSO, 2004).

These efforts have been integrated into changes in professional standards within the accounting profession as it relates to audit engagements. The current professional standards promulgated by the American Institute of Certified Public Accountants (AICPA, 2007) described internal risk in terms of two identifiable components: (1) inherent risk (IR) – the susceptibility that an account or class of transactions contained within the financial statements or underlying records could be materially misstated, either individually or when aggregated with other misstatements, and (2) control risk (CR) – the susceptibility that an "inherent risk" misstatement could occur and not be prevented or detected by the internal control system (policies and procedures) established by the corporation (AICPA, 2007).

These two components when considered together form what may be labeled "Risk of Material Misstatement" (RMM) – the professional assessment of both inherent and control risk when determining the planning, completion and conclusion of an audit engagement. However, RMM is only one aspect of the issues involved when professionals are associated with services that involve risk and describes the risks from the perspective of the corporation and not the accounting professional. The CPA is not able to directly manage IR and thereby control it since it is a function of the inherent nature of an account (such as cash) and/or classes of transactions (such as Internet-based sales). Equally important is that the CPA is not able to manage (and thereby control) CR since it is the result of decisions, policies, procedures and the resulting environment in which events and activities are recorded in the general ledger system and are the underlying documentation for summarized data in the financial statements created by the board of directors and management. However, the CPA should be able to evaluate the adequacy of the client's efforts to create a reasonable internal control environment that will address adequately the IR in their financial reporting system (AICPA, 2007).

Fraud Detection

The theft of economic (proprietary) data is a form of fraud. The importance of fraud is viewed in the context of negligence. Two degrees of negligence are important in understanding of it in relation to audit risk and fraud: ordinary negligence or the lack of reasonable care when performing services, and gross negligence or a lack of even minimum care when performing

services. The profession view is found in AICPA (2007) where fraud is defined and described as an:

> Intentional act by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception to obtain an unjust or illegal advantage. Two types of misstatements resulting from fraud are relevant to the auditor's consideration in a financial statement audit: misstatements arising from fraudulent financial reporting and misstatements arising from misappropriation of assets.

In the AICPA (2007) the responsibility to be assumed by the auditor:

> Although the auditor has no responsibility to plan and perform the audit to detect immaterial misstatements, there is a distinction in the auditor's response to detected misstatements depending on whether those misstatements are caused by error or fraud. When the auditor encounters evidence of potential fraud, regardless of its materiality, the auditor should consider the implications for the integrity of management or employees and the possible effect on other aspects of the audit.

The accounting profession attempts to use these definitions when assessing audit risk, determining DR (TD and AP) and determining the implications (effectiveness) of a client's internal control system (IR and CR) which should be designed to provide reasonable assurance regarding the achievement of objectives" as described by COSO in its 2004 framework: (1) effectiveness and efficiency of operations, (2) reliability of financial reporting, and (3) compliance with applicable laws and regulations (COSO, 2007).

DISCOVERY OF ECONOMIC THEFT WITHIN AN INFORMATION SYSTEM

The accounting professional has minimal guidance as to how auditors should gather evidence to form the basis for their report which will be issued with a client's audited financial statements. Three common approaches utilized by CPAs and learned from experience by some of the researchers are: (1) auditing around – the easiest and more common approach used within the profession is to compare known inputs with outputs generated by a client's information system, (2) auditing through – the more difficult approach for CPAs to use since it requires a level of in-depth knowledge about information systems and technology that most CPAs do not possess nor do they have the technical expertise to obtain the level of understanding of technical (electronic) control procedures in place by the information system, and (3) auditing with computer aided tools or the practice of using computer technology to automate and/or simplify the audit process (Wikipedia, 2007). The implications for the accounting profession to continue to select the more traditional approach (auditing around the computer) raises the question as to whether or not CPAs are adequately evaluating their audit risk (AR) and the detection risk (DR) component correctly during planning for a financial statement audit, and, thereby, actually increasing their exposure to claims of gross negligence and fraud.

Economic Theft via Circumvention & Fraud Risk

In general one may assume that in today's environment a business will use technology. In fact, the level of usage is described by Montague (2007) as "90% of all records are now maintained in electronic format and 70% of those are never printed out in hard copy." One aspect of evidence gathering by the CPA during a financial statement audit is to gather evidence to form an opinion on the likelihood of Internal Risk Levels One and Two policies and procedures being circumvented by one or more individuals including individuals on the board of directors, executive management and/or other personnel. The awareness of any circumvention efforts must be of interest to management and the CPA since the corporate environment of today includes a networked information technology (IT) professional unit that utilizes virus scanning tools, firewalls, network operating system features to manage the access to the company's system. However, typically IS efforts are focused on the use of well-known tools or procedures such as matching user names to passwords and the use of firewalls to reduce the intrusions by hackers.

Equally important to the internal efforts under COSO business guidelines is the ability of IS to know how to prevent and when necessary to detect errors or irregularities. That ability and effort must be coordinated with the efforts of the external auditor. In today's network environment the EA has a level of an understanding of intrusion tools useful for those engaged in fraudulent activities as well as effective methods detect the misuse of these tools. The EA attempts to find the use of techniques and tools that can be used to circumvent existing security procedures in a computer-based information system and enable unauthorized access to individuals that may wish to obtain company information-data and/or cause malicious harm to the networked system.

Economic Data Theft Caused by Employees in the Organization (Insiders)

When hackers first try to hack into an organization's networked system, they want to get access to an administrative account which would allow them to access any part of the system. Barring this, they want to compromise an account on the system from which they will try to elevate their privileges. An employee working for the organization usually already has an account on the system. Depending upon their job in the organization, this may even be an administrative account. Thus, if the employees are so inclined, they have an advantage over outside hackers—they already have approved access accounts on the organization's system.

There have already been many instances of insiders attacking an organization's information system. Insiders are typically disgruntled workers and their motives are to hurt the organization (although some have profit motives). The disgruntled workers may have been fired, laid off or may continue to be employed by the company. For some reason, they are not happy with the organization. They may be upset even if they think they are going to be laid off or fired. It is up to security professionals and management to manage disgruntled workers. Make sure the organization has an "…effective grievance procedure" (Admin, 2007). If an employee is complaining openly about something in the organization, management should know about this.

They may want to steal corporate data or plant malicious software on the network. Passwords for critical servers have been reset and were not given to the organization for days. Logic bombs that could have wiped out data on 70 servers have been planted by disgruntled workers (Judi,

2008). A contractor working at Fannie Mae is accused of planting a time bomb on its servers. "It was only by chance that (another administrator) scrolled down to the bottom of the legitimate script to discover the malicious script" (Lemos, 2009). The malicious script was hidden in the legitimate script (Lemos, 2009). This may have been avoided if Fannie Mae used a monitoring system that logged when files are modified (such as Open Source Tripwire ® (Sourceforge)). Also, some organizations are "…implementing file integrity monitoring as a source of configuration control" (Tripwire, 2009).

Passwords are often used to protect sensitive corporate data. So it is especially important for the organization to make sure secure passwords all always used by employees. If employees use secure easily cracked passwords, the login process can be easily changed to make the passwords more secure (Magruder, Lewis, & Burks, 2007). If the organization offers public access to their web servers (such as may occur in an e-commerce environment), additional problems may occur. "Security issues and threats in the e-commerce environment are varied and can be caused intentionally and unintentionally by insiders and outsiders. Many experts believe that insiders create the majority of the security threats and issues" (Bidgoli, 2003).

In a survey commissioned by Symantec in 2009, business organizations indicated they were worried that employees leaving the organization may take information from the organization that is confidential (Mills, 2009).

> The survey also found that many companies seem to be lax in protecting against data theft during layoffs. Eighty–two per cent of the respondents said their employers did not perform an audit or review of documents before the employee headed out the door and 24 per cent said they still had access to the corporate network after leaving the building (Mills, 2009).

It is critical that the organization audit its information system when a disgruntled worker is identified.

Economic downturns may affect workers ethics, according to Michael Krigsman (2009). In his article, "IT ethics and the recession", he reports on a survey by Cyber-Ark of 600 workers. The interviewed employees were from three countries, the Netherlands, US and UK. "Once workers learn they may be targeted for downsizing, their ethics may erode. Employers should be aware of this and enhance security accordingly" (Krigsman, 2009, p.4). There are many ways an employee can harm an organization. Lippert and Swiercz (2007) argue "that a user's willingness to share sensitive information on a voluntary basis", on the Internet, " is an area of concern." If an employee is not happy with the organization, will they become more or less willing to share sensitive information on the Internet about themselves or their company? As their article indicates, more research about this "willingness" is necessary.

Efforts to comply with current (and future) regulations/laws and to ensure the security of data are enhanced by log file management (Howarth, 2009). Every computer has at least one log file. Desktop computer systems have a log file. Servers have log files of users logging into their

company accounts. They may also have logs for Web servers, database servers, etc. Some systems have logs of individual user activity (a history of commands they executed). Internal and external auditors, and security personnel must monitor these logs.

One question is, "How much should employees be monitored?" One answer is to monitor everything an employee does. "RIM chief information officer Robin Bienfait, during an interview with ZDNet.com.au in Sidney, said that all actions carried out on RIM's internal network were logged, which means that people who wanted to carry out private conversations might want to bring in personal devices…. When asked exactly whether it was conversations, rather than just written information she kept tabs on, Bienfait answered: 'Everything. I record everything' " (Tindal, 2009).

There are many types of malware that the company (management, internal and external auditors) must check for that can "leak" company data. Although no port-knocking (Krzywinski, 2003; Magruder & Lewis, 2005) trojan programs have been found in the wild, code samples do exist (Mullins, 2009). Steganography (Wikipedia, 2009) can also be used to hide company data that is being "leaked" to the outside. Corporate espionage can be done by viruses written specifically for espionage (Magruder & Lewis, 1992). There are so many ways for a disgruntled worker to get company data and use the network to get the data outside of the company.

Understanding the potential existence of such tools and their usage is important to financial statement auditors and specialized auditors such as fraud examiners and forensic accountants who are engaged to determine the nature, level and implications of activities which are suspicious of being fraudulent including the inappropriate use of company assets-resources including economic data. Numerous intrusion techniques (or tools) have been identified as tools for circumvention efforts.

MANAGEMENT RECOMMENDATIONS

Several recommendations can be gleamed from the current research that are useful to management, IS personnel and the internal and external auditor functions. Recommendations specific to management are presented here. In Appendix 1 is a checklist that can be used by the internal and external audit functions and is cross-referenced within this list of recommendations. Garrison and Roderick (2006) also provide a checklist for non-security professionals who may not have a technical background.

1. Educate users about password security. Enforce secure password selections either through the system or a password generator. This should be done as part of a new employees training and also repeated every quarter and when employees leave the organization. Employees should be reminded not to let others use their organizational accounts.

2. Develop a policy regarding employees whose behavior changes. These employees may say things against the company to other employees. Their immediate supervisors may notice this as well. Develop a way for employees to let the organization know about unusual activity by other employees.

3. Develop a policy regarding employees that may be laid off or fired. Either keep them off the organization's system or monitor everything they do on the system.

4. Use a check list of actions to be taken when an employee is laid off, fired or is disgruntled. An example checklist is given in Appendix A.

5. Develop a policy regarding "user-developed" programs. Make sure the organization knows about these.

6. Consider using programmable locks on doors to sensitive areas. These are easily changed when an employee leaves the organization. A system that records access is also important.

7. Develop policies regarding taking work home; laptops, CDs, DVDs, memory sticks, etc. Minimize these actions. This should be allowed only when really needed and the employee's immediate supervisor must be advised of this and make a record as to what is being taken out of the organization.

8. Periodically check all IT policies to make sure they are up-to-date and are being enforced.

9. Have a specific email policy and monitor disgruntled workers email or discontinue their email privileges.

10. Monitor disgruntled employees.

11. Consider that a Distributed Denial of Service attack may be a cover for an attack. It may be used to "clog up" the logs to hide a disgruntled worker's attempt to get back into the system.

12. Check all logs periodically (volume determines how often) and especially after an employee has left the organization. In Windows XP, the log is called "Event Log" and is viewed in the "Event Viewer"

13. Use a log analyzer. This will help the organization in finding any "leaking data" and help it to make sure no disgruntled workers are getting back into the system.
14. Have the technology department check the company's firewall settings to make sure they are up-to-date.
15. Use a system that monitors files. This also helps with compliance with federal laws.

CONCLUSIONS

Several types of risk are considered by a business and its external auditor including the two traditional perspectives of internal and external to the company. However, these risk factors continue to change due to changes in the global marketplace. A disconnect between the external

auditor and the IS in-house staff is a concern. Continual coordination and exchanging of information is necessary if a business and its external auditor are to effectively manage the risk related to the theft of economic data by employees. Checklists are provided to help management, the internal auditor and external auditor to help to manage the risk of employees taking company data, exposing the company to legal issues, loss of "good will" and compliance issues.

REFERENCES

Admin. (2007). Insider hacking is serious business, *FierceCIO,* April 26, 2007, http://www.fiercecio.com/story/insider-hacking-is-serious-business/2007-04-27. Accessed 27 February, 2009.

AICPA. (2005). Audit Committee Toolkit, Internal Control: A Tool for the Audit Committee.

AICPA. (2005). The AICPA Audit Committee Toolkit, 2005, Basics of Internal Control," 1.

AICPA. (2007). Professional Standards, Vol. I (July 7, 2007), AU 312, 257-261.

Bidgoli, H. (2003). An Integrated Model For Improving Security Management In The E-Commerce Environment. *Journal of International Technology and Information Management,* 12(2), 119-134.

COSO. (2004). Committee of Sponsoring Organizations of the Treadway Commission, Enterprise Risk Management Executive Summary, September 2004, pages v - 2.

COSO, (2007). Committee of Sponsoring Organizations of the Treadway Commission, Internal Control – Integrated Framework - guidance on Monitoring Internal Control Systems, Discussion Document, September 2007, page 3.

Garrison, C. P. & Roderick P. (2006). Computer security checklist for non-security technology professionals. *Journal of International Technology and Information Management*, 15(3), 87-91.

Howarth, F. (2009). As crunch bites: Don't neglect the logs. http://software.silicon.com/security/0,39024655,39391737,00.htm, 5 February 2009. Downloaded 27 February 2009.

Judi, FierceCIO. (2008). The Exceutive IT Management Briefing, Disgruntled workers may attack security. Oct 15, 2008. http://www.fiercecio.com/story/disgruntled-workers-may-attack-security/2008-10-15. Downloaded 27 February 2009.

Krigsman, M. (2008). IT ethics and the recession. December 23, 2008, http://blogs.zdnet.com/projectfailures/?p=1196. Downloaded February 26, 2009.

Krzywinski, M., (2003). Port Knocking Network Authentication Across Closed Ports. *SysAdmin Magazine,* 12, 12-17.

Lemos, R. (2009). Security Focus, Contractor indicted for Fannie Mae malware. http://www.securityfocus.com/brief/897, January 30, 2009.

Lippert, S. K, & Swiercz, P. M. (2007). Personal data Collection via the Internet: The Role of Privacy Sensitivity and Technology Trust. *Journal of International Technology and Information Management*, 16(1), 17-30.

Magruder, J. S. & Lewis, S. X. (1992, January). Espionage via Viruses. *Computer Fraud & Security Bulletin*, 14-16.

Magruder, S., Lewis,S. X. & Burks, E. (2007). More Secure Passwords. *Journal of International Technology and Information Management*, 16(1), 87-96.

Magruder, S., Lewis, S. X. & Chen, K. L. (2005). Sending Messages Via Port Knocking. *Information Resources Management Association International Conference Proceedings;* San Diego, California; May 15-18, 2005; 1214-1216.

McMillan, R. (2009). With economic slump, concerns rise over data theft. *IDG.net* Story, International Data Group, 2009.

Mills, E. (2009). Disgruntled workers pocketing company data on their way out.http://www.silicon.com/research/specialreports/protecting-enterprise-data/disgruntled-workers-pocketing-company-dat-on-their-way-out-39398405.htm, 24 February, 2009.

Montague, B. A.(2007). Report from Counsel – Comments on Recent Legal Developments and Trends from Law Offices of Brian A. Montague, PLLC. *Navigating Electronic Discovery Rules*, Fall, 4.

Mullins, M. (2009). Be aware of potential threats from port knocking. http://techrepublic.com.com/5208-6230-0.html?forumID=4&threadID=177189&start=0, downloaded 25 February, 2009.

Sarbanes-Oxley. (2002). http://www.soxlaw.com/

Sourceforge, Open Source Tripwire ®, http://sourceforge.net/projects/tripwire/

Tindal, S.(2009). ZDNet.com.au, RIM records all employee calls. http://news.zdnet.com/2100-9595_22-275216.html, downloaded March 4, 2009.

Tripwire. (2009). How Educational Institutions Use File Integrity Monitoring to Achieve PCI Compliance. email sent to an author regarding a Webcast on March 11, 2009, presented by Ed Rarick.

Treadway Commission, (1992). *Internal Control—Integrated Framework*.

Wikipedia. (2007). Computer Aided Audit Tools. http://en.wikipedia.org/wiki/Data_analysis_(information_technology)

Wikipedia. (2009). Steganography, http://en.wikipedia.org/wiki/Steganography , downloaded 9 March 2009.

Appendix A

Checklist

Internal Auditor

❑	All passwords that the employee used or had access to are changed.
❑	The employee's computers on the company's network have been isolated.
	The employee's computer has been examined for
❑	unusual configurations, programs,
❑	backdoor programs,
❑	time/logic bombs,
❑	port-knocking programs (programs that can "leak" company information),
❑	steganography programs,
❑	malware, etc. Note anything found.
❑	The employee's server account have been isolated and examined. Note anything found.
❑	Physical locks employee had access to have been changed.
❑	Employee's office and desk locks have been changed.
❑	Scripts/programs the employee wrote or had access to or used have been examined.
❑	Remote access for the employee has been removed.
❑	Check computer logs
❑	Server logs Note unusual activity:

❑	Web logs Note unusual activity:
❑	Employee's desktop logs Note unusual activity:
❑	The employee's name has been removed from all access lists.
❑	The network has been checked for unauthorized account(s) the employee may have created (backdoor).
❑	A log analyzer is in place and being used.
❑	The firewall settings for the company's network have been checked.

External Auditor

Checklist

❑	A secure password policy is in place.
❑ Date:	What was the date the last time a company computer account was compromised?
❑	The company's computer log files are checked periodically by the technology employees.
❑	Check the company's server log files.
❑	The company has in place a "disgruntled worker" policy.
❑ Date:	Date the last time the "disgruntled worker" policy was needed.
❑	File monitoring is in place and the generated logs are checked.
❑	Is there evidence that the Internal auditor consistently is using a checklist similar to the one given above?