Security Threats: Auditors and Technology

Houston H. Carr
Auburn University
Alumni Professor Emeritus, College of Business
129 Quail Lane
Dadeville, AL 36853-4931 USA

Denise J. McManus
The University of Alabama
Information Systems, Statistics, and Management Science Department
Culverhouse College of Commerce
Box 870226
Tuscaloosa, AL 35487-0226 USA

Nicole Gué
Auburn University
129 Quail Lane
Dadeville, AL 36853-4931 USA

Abstract

Technological advances, data security breaches, and unethical auditors pose a significant threat for organizations partnering with public accounting firms. Information acquired during an audit has significant value in the marketplace, i.e., it can be sold. Threats from the auditing process may be the intentional or unintentional misuse of data; however, the end result for the organization's long term viability can be disastrous. Protecting sensitive data, managing an effective audit and minimizing security threats are key components of a successful corporation. We will discuss how companies can effectively manage this process while minimizing risk to the organization's valuable information.

Keywords: Audit, Data Security, Security Threats, IT Audit

1. Data Security Audit

Corporate data contains sensitive and proprietary information. Big Four accounting firms have thousands of employees all over the world that have access to their customer's data, with theresponsibility to keep it secure. Historically, accounting methods of control, such as segregation of duties, have provided checkpoints of data entry and record keeping.Computer-based and media processing have introduced new challenges to controlling accounting and auditing practices. These challenges are direct resultsof computers, networks, and the internet usage, causing security risks. Security threats are introduced when an organization goes through an audit due to the nature of an audit. This formal examination of corporate accounts and financial records requires the release of data to the accounting firm conducting the audit. Furthermore, it is common practice to outsource smaller audits to third parties in foreign countries.

Intentional or unintentional data theft by ethical and unethical auditors is a growing trend; motivation for an auditor to steal sensitive data is directly related to the potentially enormous financial profit made from the transaction. "Today, the biggest security threat facing an organization is internal, and companies have a bottom-line need to protect both their customers and their business from data privacy breaches. Even if a company has a plan in place to prevent unauthorized users from accessing data, it needs a solution that provides insight into the actions of trusted users" (Application Auditing, 2007).

Significant losses of customers, clients and patients could be the direct result of failure to protect personal and organizational-sensitive information. Moreover, the results of the data security breach could include the loss of organizational revenues and future clients in addition to the significant expense of required notification and recovery.What are the threats?

2. Security Threats

Security must be an overriding issue for all organizations. Simply put, how can we be concerned with knowledgeif it is not in an environment of security and privacy; how can we support management if it is not done in an atmosphere of ethics. Carr (2009, 2004, and 1992) and othershave performed research in the nature of security and its changing focus in the United States over the past two decades. In each case, they asked IT/IS/Security professional to rate the importance of various threats. The results of the research listing the top five threats are shown in Table 1.

While the respondents did not indicate these were failures of application ordata/knowledge base creation, it is obvious that these threats are specifically aimed at vulnerabilities of such applications or stores. Because of the threat to privacy in particular, the government of the United States and others have enacted specific laws and regulation to provide security of data in IT systems and during transport. From GLBA to SoX to HIPAA to state laws, the concern for protection of personal data is a topic of great concern.

2.1 Source of Threats and Methodology of Protection.

There appears to be two primary organizational considerations; (1) the security of application, storage, and (2) the transport and methodologies of protection. Figure 1 shows the three points of vulnerability to security threats. Of concern is whether the security and privacy measures are incorporated at the time of creation or are they added later. Even ignoring the added cost of later incorporation, e.g., pay me now or pay me later, the system analysis would not be complete without understanding the security vulnerabilities and threats.

Security Threats Research (Top 5 Threats)		
Carr, McMicken, & Brooks, (2009)	**Carr & Dugan, (2004)**	**Loch, Carr, & Warkentin, 1992**
1. Data compromised	1. Viruses	1. Natural Disasters
2. Failure to use firewall and filters to secure access from public	2. Unauthorized access by hackers	2. Accidental Entry of Bad Data by Employees
3. Unauthorized access & Use; lack of authentication	3. Network failure	3. Accidental Destruction of Data by Employees
4. Improper maintained/secured laptops.	4. Unauthorized access by employees	4. Weak or Ineffective Controls
5. Poor encryption/password use and policies	5. Utility failure	5. Entry of computer Viruses

Table 1 Security Threats Research

Figure 1 indicates that threats come from inside and outside of the perimeter/organization.Security may be included in three methods. Considering that threats from inside were mentioned in each of the three studies, the question of management policy seems critical. Yes, the applications and stores must be hardened through architecture and with the use of proper technology, but it is the application of management policy that adds even greater strength. This includes such issues as *least privileges* and *separation of privileges.*

2.2 How Threats have changed over two Decades

The nature of the IT environment and threat concerns have changed over the past two decades. *Mother Nature* was the highest ranked threat by far in 1992 due to recent weather incidents and the immature but evolving methods of protection. The *acts of users* came in a fairly close #2 and #3 and remain of concern through many diverse surveys. In 2004, the security of the network and its connection to the outside world rose to the top. This is likely due, in part, by the popularity of the World Wide Web and the evolving nature of hackers. This trend continues in 2009, even though the original questions that resulted in the elements of the 2009 survey were a part of research into the nature of threats to wireless environments. It has been during the latter half of this decade that the news abounds of corporate network/stores intrusions and lost unsecured laptops. It is fairly easy to postulate that this change has come about due to the maturity of and dependence on networks, in general, and applications that attached to the Internet via wireless capabilities, in particular. As the world became connected, organization and individuals became accessible targets.

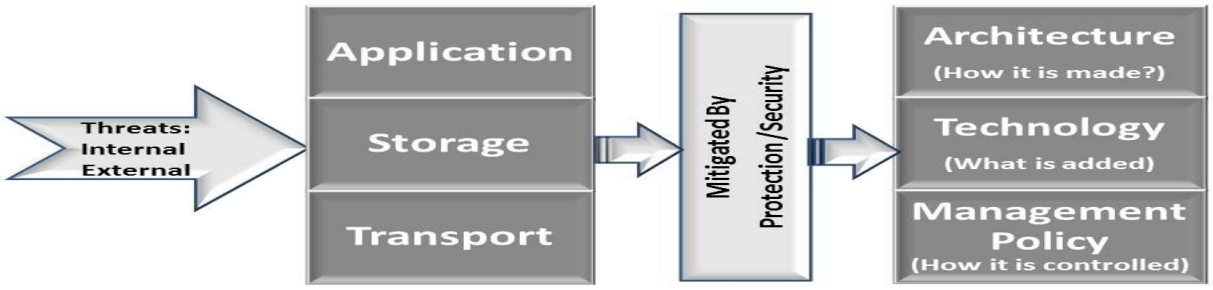

Figure 1 – Protection against Threats

3. Auditor Security Threats

The basic tenant is that information has value; it can be sold and/or used in competition. Data theft of sensitive information by malicious hacker attacks against banks and credit card companiesalso breach the trust of clients. Auditors have access to an organization's financial, sales and distribution, customer, and supplier records. Malicious activities such as the collection of data relating to the customer base of a retail company could be sold to competitors. Examining frequent vendors and possibly even calling them to confirm transactions could provide information about a new drug of a pharmaceutical company. The harm an auditor could intentionally do to the business is significant.Jamie Hopper, a controller with Georgia Pacific, agrees, Auditors "have access to basically your entire systems, including customer and financial systems. An auditor could derive basically anything they wanted to know from very valuable information (i.e. margins, profits, prices, etc.)."

Perhaps more dangerous are the unintentional threats caused by careless auditors. Social networking sites were the number one security topic for 2011.

"With a 13% increase in identity fraud between 2010 and 2011, a study conducted by Javelin Strategy & Research showed that consumers may be putting themselves at a higher risk for identity theft as a result of their increasingly intimate social media behaviors. Sixty-eight percent of people with public social media profiles on platforms such as Facebook or Twitter shared their birthday information with 45% of them getting into specifics about the exact month, day, and year. Sixty-three percent shared where exactly they attended high school. Eighteen percent shared their phone number and 12% shared their pet's name. Not only are all of these details typically asked when verifying an identity, but people also frequently use them in passwords. The statistics are clear — people are giving away far too much personal information on social networking sites, allowing for fraudsters to easily steal their identities.(Black, 2012, p.1).

The 2013 identity fraud study reports that in "2012 identity fraud incidents increased by more than one million victims and fraudsters stole more than $21 billion, the highest since 2009 (Javelin Strategy, 2013).*Facebook* and *Twitter* may be blocked in the office, but what happens when an auditor is working on their computer in a coffee shop, either on duplicated organization data or connected to the organization database? Hackers are using an application called Fire sheep to hijack the social networking session of a user at a nearby table. If the session happens to contain sensitive information, the hacker now has the information (Rai & Chukwuma, 2011). Other methodologies for interception of such data are man-in-the-middle (MITM) attacks and key logging. A MITM attack occurs when the attacker uses a laptop to act as a wireless access point and read the data as it passes onto the legitimate access point. Key logging can be done from anywhere; it is a process of installing a program on the auditor's computer that records key strokes and sends them to the attacker. This bypasses security since the actual keystrokes are recorded and passed to the hacker.

About two-thirds of an organization's sensitive data is on endpoints,which include desktop and laptop computers, tabletsand smart phones. Many public accounting firms give their employees PDAs, smart phones, and tablets when they begin working for them, helping to make business more efficient. Problems arise in two situations. Auditors may usethese remote devices when accessing organizational data or they may use laptop computer to hold or access the data via corporate networks.

If the employee or auditor keeps sensitive information on their laptop computerand does not have the appropriate virus, firewall and encryption protection, the sensitive information is not secure. Unfortunately, most PDAs, smartphones, and tablets do not have similar protection. Further, if they connect a laptop, PDA, smart phone, or tablet to an unsecured wireless network, a hacker could easily access sensitive information (Rai & Chukwuma, 2010).So how does a company protect itself?

"In today's global economy, service organizations or service providers must demonstrate that they have adequate controls and safeguards when they host or process data belonging to their customers" (SAS 70 Overview, 2013).The dynamic nature of the corporate environment poses challenges during the management of regulatory and security requirements, as well as professional auditing standards, disclosures and constraints.

4. Audit Protection

In 2011, organizational data breaches in the United States averaged $7.2 million each, with 31% being malicious attacks, costing an average of $318 per record (Ponemon Study, 2011).This leaves 69% of the intrusions due to non-malicious, possibly accidental access. We have evaluated and present three levels of security that we believe will benefit all organizations. These include both preventative and after-the-fact techniques.

4.1 Security Level I – Data Loss Prevention

Data Loss Prevention (DLP) stops information from leaving the organization's office. DLP identifies, monitors and protects confidential data on networks as well as storage and endpoint devices. It is built into the information system and controls access to different interfaces. It does this by recognizing software agents installed onto a computer, smartphone, tablet, or PDA. Basically, it sets boundaries for each user of the information system—a preventative measure (Rai & Chukwuma, 2010).Detection and prevention of unauthorized access to the data are key strategic components of DLP on all types of data, i.e. network, stored, shared.

"In a perfect world, there would be no need to hand over sensitive data to [third-party] agents that may unknowingly or maliciously leak it……in a perfect world we could watermark each object so that we could trace its origins with absolute certainty. [In an imperfect world], data allocation strategies (across the agents) improve the probabilities of identifying leakages...detecting the leakage and identifying the guilty party"(Papadimitriou & Garcia-Molina, January, 2011).

4.2 Security Level II – Application Auditing Solution

Compuware's Application Auditing Solution is designed to stop security problems caused by internal, authorized users. It records users' activities, creating an after-the-fact audit trail. Because it is directly connected to the main operating system, it can record more than eight million transactions per day. If a security problem occurs, the program is able to identify the offender. Malicious acts could be prevented by informing all auditors and employees of this program (Application Auditing, 2007). Larry Ponemon, Chairman and Founder of the Ponemon Institute says, "Our research shows that insider threats represent one of the most difficult management challenges for data security and privacy professionals. Detecting, deterring and mitigating the insider threat within a complex organization cannot happen without using enabling technologies like Compuware's application auditing solutions"(Application Auditing, 2007). Software lets organizations capture activity between authorized users and applications, providing an audit trail that can be used to investigate security breaches and pinpoint affected customers to reduce potential impact (Ponemon Study, 2011; Application Auditing, 2007).

4.3 Security Level III - Full Disk Encryption

Protecting data on endpoint devices may require full disk encryption (FDE).Full disk encryption converts all information on the device into unreadable code, thus, preventing a breach of the data even in the case of unauthorized access. Lost or stolen devices/endpoints are protected by this encryption method, thus, providing the highest level of security for all corporate intellectual property.FDE is becoming a standard technique for laptops due to the loss of 200,000 laptop computer a year, many containing unencrypted organizational data. However, for the audit to be conducted, the auditor must have access to unencrypted data.While FDE protects the data from unauthorized access, it does not protect it from malicious or careless auditors and that data used in the open; e.g., mobile devices used in public places.

4.4 Audit of the IT Function

Due to increasing concern about security, the SAS 70 auditor[1] has appeared. The statement on Auditing Standards (SAS) No. 70, Service Organizations, recognizes that a service organization has been through an in-depth audit of their control objectives and control activities, which often include controls over information technology and related processes (Bell, 2010; SAS 70 Overview, 2013).This auditor "audits annually the IT and business processes and procedures that affect its customer's business"(Leung, 2003, p. 1). These auditors are technologically-savvy and are purposefully gaining knowledge about an organization's security functions. Ironically, this may make them even more ableto take advantage of this trust.(Leung, 2003).

5. Summary and Conclusions

Organization will continue to receive bad press when intrusion occurs; this can only lead to loss of customers. The concern over personal information privacy has become a vital concern as governments establish significant penalties for intrusion, theft, and even loss of such information. The world is, indeed, information- and knowledge- based; it is also access-based. Without secure applications, stores, and transport, we lose confidence and organizations lose their most valuable asset, their reputation and customers.

Most organization work on the assumption that auditors are bound by professional standards and, therefore, pose no security risk. What if they are wrong and auditors *are* threats to the companies that hire them. They may intentionally steal data or unintentionally make data unsecure. While new technology will hopefully offer more ways for companies to protect themselves from outsiders, including their own auditors, ever vigilance is the price of security.

[1]"Statement on Auditing Standards (SAS) No. 70, Service Organizations, is a widely recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA). A service auditor's examination performed in accordance with SAS No. 70 (also commonly referred to as a "SAS 70 Audit") is widely recognized, because it represents that a service organization has been through an in-depth audit of their control objectives and control activities, which often include controls over information technology and related processes" [http://sas70.com/sas70_overview.html].

References

Application Auditing Solution Offers Risk Management by Compuware Corporation, (2007), Transmission & Distribution World (Online Exclusive), Prism Business Media. http://tdworld.com/smarter-grid/application-auditing-solution-offers-risk-management

Bell, T. J. (2010). Synthesizing SAS 70 Audits and PMIs Project Management Process Groups: Using Project Management Principles to Optimize the SAS 70 Auditing Process. ISASCA Journal, 4, 1-8.

Black, R. (2012). Credit Report.org "9 Alarming Statistics About Identity Theft", accessed 4/25/2013; (http://www.creditreport.org/9-alarming-statistics-about-identity-theft/)

Carr, H. & Dugan, J. (2004).Information Systems Security: Revisited. Unpublished manuscript, Auburn University.

Carr, H., McMicken, T. & Brooks, L. (2009).Information Systems Security: Two Decades of Threats. Unpublished manuscript, Auburn University.

Leung, L. (2003). Call in the Security Auditors: Independent SAS 70 audits could show you how secure data is with your service provider. Network World, Inc., July 28.

Loch, K. D., Carr, H. H., &Warkentin, M.E. (1992). Threats to Information System Security: Management's Perceptions Reflect Yesterday's Environment. Management Information SystemsQuarterly, 16:2 ,173-186.

More than 12 Million Identity Fraud Victims in 2012 According to Latest Javelin Strategy & Research Report, (2013), Javelin Strategy & Research Report. [Online] Available:https://www.javelinstrategy.com/news/1387/92/.1

Papadimitriou, P. &Garci-Molina, G. (2011).Data Leakage Detection. IEEE Transactions on Knowledge and Data Engineering, 23(1), pp. 51-63.

Ponoemon Study Indicates Organizational Data Breach Costs Hit $7.2 Million and Show No Sign of LeveleingOff. (2011). Symantic Corporation Press Release. [Online] Available: http://www.symantec.com/about/news/release/article.jsp?prid=20110308_01

Rai, S. &Chikwuma, P. (2011).2011 Top Security Topics: As New Threats Emerge, Auditors need to put Technologies such as Social Networking and Smart Devices into this Year's Audit Plan.Internal Auditor, April 1.

Rai, S. & Chukwuma, P. (2010). IT Audit-Beginning at the endpoint: faced with an ever changing mix of new technologies, auditors should make these devices the starting point in security reviews,Internal Auditor, June.

SAS 70 Overview, (2013). [Online] Available :(http://sas70.com/sas70_overview.html).