System Audit: Looking for Ways to Control Security Issues

John W. McClain

East Carolina University

Abstract

Protecting company assets, privacy and employees is vital for companies operating in a hyper connected world. The number of products and services designed to provide security seem to multiply on a daily basis. Obviously, the need to secure the lines of communications that allow business and individuals to come together in a mutual exchange of products and services are very important to everyone. But, the increased number of security incidents and hacks seem to coincide with the proliferation of security products. The purpose of this paper is to discuss why some of these incidents continue to occur and a lot of them involve the same scenario. The usual reason for issues are product rush to market, change control process not followed and historical systems that have flaws but still being used by companies. One area that would help a lot of companies is to conduct better IT Audits. The process is similar to risk assessment but with an emphasis on the total system with more frequency. The risky environment that companies are operating in today requires timely information. This paper will discuss using continuous auditing concepts for security.

Information technology is what makes the world work. A great example is the raise of smartphone technology. Smartphones makes it easier to keep in contact with anyone or thing that's important. Smartphone technology isn't the only area of explosive growth but smartphone technology is a great example of smaller, faster and power being used to make communication and work easier. For instance, the screens on most of these phones have great screen resolution in some cases the resolution is better than personal computers. So, small devices with a lot of power that are easy to use are creating excellent platforms for users. Another factor is the number apps that give users the ability to check email, conduct online banking to include deposit checks and play music in some cases are developed for these. The car company Tesla issued a fix for their cars via wireless links while GMC is having people schedule appointments in repair shops for repairs due to a recent vehicle recall (Brisbourne, 2014). This is a great customer service tool but a lot of pressure is created on making sure this power isn't abused. Storing and securing this information is something that needs to be monitored constantly. Most of this data is stored in the cloud. Cloud computing is making it easier to store huge amounts of information out of the confines of the normal data center setup. High speed WAN links is making it easier to off load the costs of huge datacenters because large amounts of data and processing power is available due to cloud computing. This information is traversing various links that go through some areas that aren't very hospitable and aren't concerned about confidentiality, integrity or the availability of the data. These hostile areas aren't defined by location but the ability to individuals to tap into weak links and unprotected areas that will give them the opportunity to access data. The pervasive nature of information technology means that these tools that come in a variety of forms must be protected from individuals that would like to use these tools for nefarious objectives. The ability to protect sensitive assets would be easier if hackers were the only problem. Unfortunately, that's not the case. Employees may have an issue with their treatment or would like to gain something from the sale of information. The volume of information and the number of devices accessing the data is another problem. The devices that transport, store and work on the data are subject to mistakes in setup, mistakes in system updates and replacement. The inability make simple changes to default passwords create an easy to exploit vulnerability. The issue of default passwords should be an easy check for installers of network equipment. The United States computer emergency response team issued alert TA13-175A concerning the risk of default passwords on the internet. The following examples where listed in this alert (US-CERT, 2013).

- Internet Census 2012 Carna Botnet distributed scanning
- Fake Emergency Alert System (EAS) warnings about zombies
- Stuxnet and Siemens SIMATIC WinCC software
- Kaiten malware and older versions of Microsoft SQL Server
- SSH access to jailbroken Apple iPhones
- Cisco router default Telnet and enable passwords
- SNMP community strings

The alert listed the following products as likely to use default passwords.

- Routers, access points, switches, firewalls, and other network equipment
- Databases
- Web applications
- Industrial Control Systems (ICS) systems
- Other embedded systems and devices

- Remote terminal interfaces like Telnet and SSH
- Administrative web interfaces

The devices mentioned in this alert are the devices and products that actually power electronic commerce. It’s hard to get a clear handle on the amount of data and the devices that hold data. The growth of cloud computing along with the pervasive nature of network access via hard to define locations is a headache. The headache is compounded by the amount of sensitive information that’s being left on devices after disposal. It’s vital for companies to take a serious look at what can be done to protect their interests. The marketing teams for security companies are constantly pushing the next appliance that will allow companies to stop all sorts of exploits but companies with the latest tools fall victim to poor planning, no over site and failure to react to issues. For example, the recent breach at Target Corporation (Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It, 2014). Target had a FireEye security appliance in place but didn’t react to alerts provided by the system according to an article in Business Week. According to the article, FireEye has a function that automatically delete malicious software but this feature wasn’t used because it’s know to for incorrectly flagging data has malware. At times this feature has been known to stop legitimate traffic like email and web traffic. These kinds of tools require a lot of time to get them setup and running properly. Even after the tools are in place monitoring needs to be done or these devices are nothing more that expensive show pieces. Charles Dormer in a journal article titled “This Should Not Be Happening” made the following statement about security (Ross, 2012):

“*IBM celebrated it centenary some months ago; commercial security consultancies and anti-malware companies are ten a penny; every software vendor provides voluminous advice on security; ISACA provides quality advice and highly qualified professionals and has developed* *schemes such as COBIT. More formal methodologies such as SABSA accompanied by standards such as ISO 2700x abound.*

We do pen testing, security certification testing, deploy 'unbreakable cryptographic schemes and we have defense and other government agencies that employ some of the best security professionals on the planet. But, an individual or group permeates through all of this stuff like a knife through better."

Mr. Dormer's makes a good point about breaches because of the number of reported incidents. Sometimes excuses are made for not being able to properly handle the alerts that are being received. In the case of target it was stated that the volume of alerts made it impossible to understand the scope of the breach. A lot of people are already concerned about these kinds of issues not just companies that are trying to protect assets. Consumers are concerned about who has access to their information. For companies the following governance issues were listed from a survey conducted by the information systems audit and control association (ISACA, A Business Framework for the Governance and Management of Enterprise IT, 2014):

- Increased security threats
- Data privacy
- Indentity/ access management
- Attacks against connected devices
- Compliance requirements
- Ownership of technology/data outside IT
- Third-party requests for data

The environment that security professionals are tasked with protecting varies in size and the avenues for compromised vary as well. The Information systems audit and control association created a document called information chaos that notes the amount of activity, risks and costs of using information. Cybercrime costs the United States 1 Trillion dollars per year (ISACA). Cybercrime has increased the need for cyber insurance policies. These policies are designed like most insurance products. When things fail the costs of bad incidents can be offset by insurance. Cyberinsurance policies were developed to offset the risk of operating in cyberspace. It’s not easy to get these policies because the companies that provide these policies want to make sure the policy isn’t viewed as a security appliance (Ward, 2014). No amount of preventive, detective and corrective controls will eliminate the threats. In 2012, there were 75 million variants of malware available. On a daily basis the average corporate worker sends and receives 112 e-mails per day. The average work receives 3 terabytes of data per year. In 2020 it’s estimated that 24 billion devices will be connected to the internet. Over 65 countries have data protection laws and various states within the United States have data protection and notification laws concerning letting individuals know personal information has been compromised (ISACA). The internet corporation for names received some push back when they wanted to update whois records. ICANN wanted to hold registrars to higher standard but the European Union is concerned about privacy protection. The EU sent a letter to ICANN stating the following (Sanders, 2014):

> *‘Taking into account the diversity of these registrars in terms of size and technical and organisational security measures, and the chance of data breaches causing adverse effects to Individuals holding a domain name, the Working Party finds the benefits of this proposal disproportionate to the risk for individuals and their rights to the protection of their personal data."*

Because the world is so connected it’s important that security be looked at more than a series to tools in place or a reaction to laws that in most cases are seen as hindrance to business doing the job or providing goods or services. The only way to react to those kinds of issues is looking at some way to make compliance is factored into the way companies conduct business. Recently, the Information Systems Audit and Control Association (ISACA) rolled out Control Objectives for Information and Related Technology (COBIT) version 5 (ISACA, A Business Framework for the Governance and Management of Enterprise IT, 2014). The goal of this tool is to make the governance and management of technology easy using broad based guidelines. The governance is part of COBIT is based upon evaluation of options, directing a broad strategy and monitoring how the strategy is working. The management side is built around four domains of planning, building, running and monitoring the progress of directives. If governance and management objectives are aligned the organization should be able to achieve the objectives set. In order to monitor progress a company needs to have a way to monitor progress. A lot of areas could be discussed or addressed but the main issues affecting companies is security problems. New attack issues based upon advanced persistent threats which mean an entity is under constant threat due to the attackers being part of groups or countries that desire to obtain sensitive information using consistent hacking attempts. Cloud computing with its' service offering are making this kinds of attacks cheaper and easier to perform. Normally, security is defined in terms of monitoring things like the number of attacks occurring or the number of attacks that are prevented but how is this information delivered. A better way to deliver information is to take the security monitoring approach and deliver the information in the form of an auditing report. Auditing is normally associated with how well a company is doing the in the compliance or financial field but with security. The reports need to be real time and based upon goals and objectives being meet in order to protect company. Failure to keep assets protected will cause problems with one of the main goals management that's to protect stakeholders interest.

The auditing process isn’t something that’s new. The roots of auditing are based upon financial and regulatory systems. In the 21st century, the use of security monitoring is sometimes viewed as auditing. Auditing focuses in assurance, risk and control issues. Monitoring a feedback tool used to make things like firewalls are operating as expected. Another thing to consider for monitoring is alerts when systems are under attack. At this time the pervasive use of technology gives companies the ability to conduct continuous auditing because most people are getting real-time data from various apps, news feeds, e-mail systems and alerting programs. Why not use continuous auditing concepts for security systems. Continuous auditing is “a methodology that enables independent auditors to provide written assurance on a subject matter using a series of auditor’s reports issued simultaneously with, or within a short period of time after the occurrence of an event” (Sarva, 2006). The same concept can be applied to security auditing. Continuous auditing needs continuous monitoring systems that are designed to feed information to so this information can be collected and evaluated on a real-time basis. This is possible because of the power and speed of today’s technology. An accounting partner made this statement about technology “Use technology to actually audit as opposed to using technology to automate manual auditing procedures” (Sarva, 2006). Advances in technology include (Sarva, 2006) (Cascarino, 2012):

- Strong processors capable of being partitioned for running parallel activities
- Disk mirroring and raid systems that provide the ability to capture transactions
- Petabytes (a petabyte is one thousand trillion bytes) of cheap disk storage
- Broadband networks delivering high speed data transfer
- Strong encryption algorithms to provide a high level of security
- Hand held devices with a lot of computing power

- Cheap data plans for handheld devices

Developing a continuous auditing program could create issues for IT auditing and security professionals. An IT audit is a rigorous and formal verification of compliance with standards, regulatory requirements, policies, processes and procedures. Security professionals normally use a risk assessment that includes gathering information to evaluate and understand the capabilities, maturity, quality, and other attributes of the thing being assessed (Freund, 2012). Another issue is the scope of an IT audit is based upon a specific scope. Security is more of an informal fluid issue that's not tied to a specific scope but tied to incidents and how to quickly fix the problem (Anderson, 2013). If both sides embrace the benefits of working together for the company issues like communication, territory and general understanding of how both areas work for the good of the company. It needs to be understood the failures by either side could lead to the following types of issues for the company (ISACA, IPv6 Security Audit/Assurance Program, 2012):

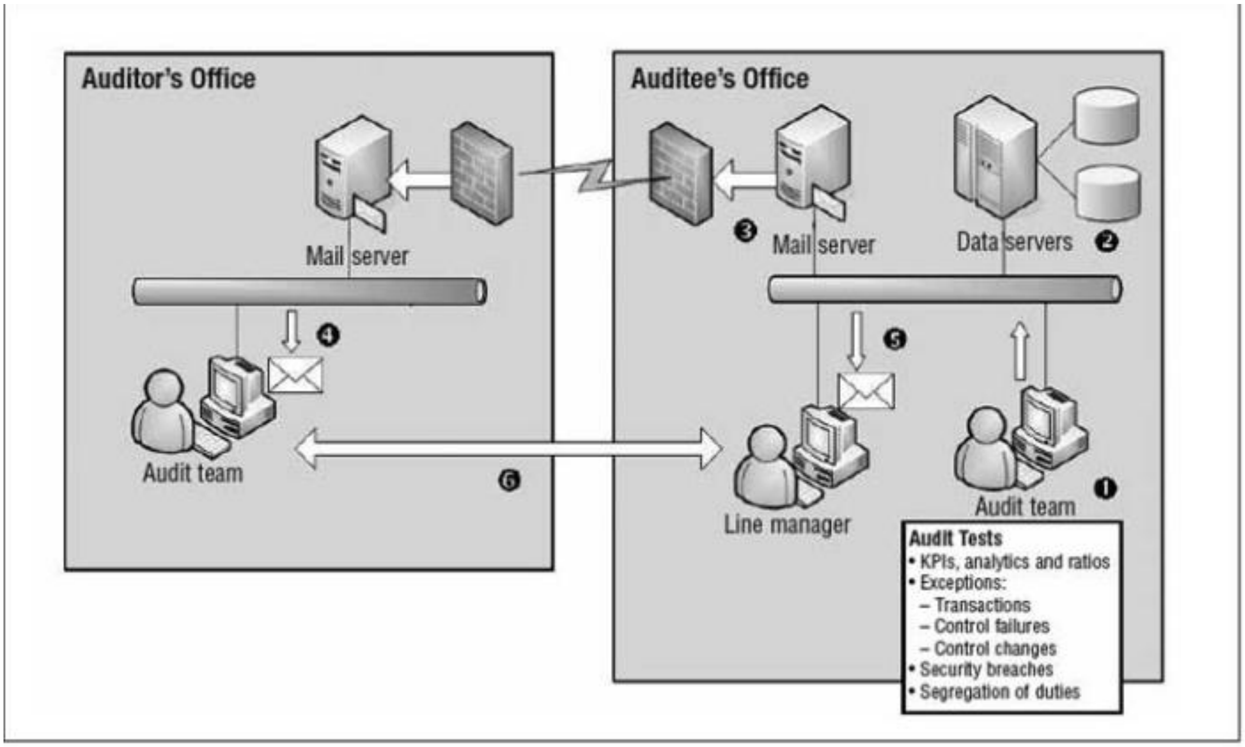
- Loss of competitive advantage
- Violation of regulatory requirements
- Disruption of network traffic
- Loss of physical assets
- Loss of customer confidence
- Network used to launch malware
- Inability to meet service level agreements
- Disclosure of privileged information
- Service outages
- Lawsuits

In order to make continuous security auditing work a few areas need to be in place (Handscombe, 2007):

- **Technology tools-**. Technology that can speed up communication is also needed, because there is no value in identifying an issue quickly if it is not communicated equally quickly to those who need to know about it. The ability to quickly alert management to security issues and failure is one the biggest multipliers that technology gives the 21st century management team. Email, paging, and network monitoring tools that can quickly alert responsible parties to problems are tools that should be enhanced. Standard communication tools like weekly, quarterly and annual security reports can quickly be delivered via electronic channels.
- **Good control environment -** Continuous auditing includes continuous monitoring and reporting by exception on problems that arise. A lot of false positive won't give the management team confidence in new procedures.
- **Senior management support -** No project is going to work without management support. So, it's important to make sure the concept is sold and buy in from the management team is solid.
- **Right of access to data -** Auditors need to have access to data on a continuous basis. Where IT management has been outsourced to a third party, the outsourcing contract should have adequate provision for audit access to data. This is one of the biggest barriers to continuous audit. An outsourcing agreement that has been implemented badly can prevent it from working at all.

- **Adaptable audit team** – One of the biggest challenges for companies is the human resource component. The team needs to be versed in security, business and auditing procedures. Another issue is the ability to communicate the finding without prejudice.

The goal is to manage the security of the systems based upon continuous auditing in order to have a better reporting framework for security issues in problems. The information security is focused on three main areas vulnerability management, security information management and configuration control and management. Real-time vulnerability is looking at issues that will require patching if required due to zero-day kinds of attacks along with the realization that patching could create some problems. Critical security event monitoring will require some type of log aggregation program that will allow the company to keep historical data but react to threats if alerted by intrusion detection devices or firewalls. The intrusion event logs must be used to identify vulnerabilities. Problems with equipment use like the one experienced by Target Corporation, in which the company had the right tool in place but failed to react to the data due to problems with problems caused by the product has to be identified. If not corrected early, the potential for security breaches creates a potential vulnerability (Santos & Pereira, 2010). Compliance failure will require some kind of trigger that's based upon defined criteria so that non-compliance alerts or analysis that shows a failure or potential for failure is quickly identified and fixed. The next figure shows a simple description of how real time problems could be reported using the e-mail system (Handscombe, 2007).



If these conceptual areas are understood, it will be easier for the company to define areas that could become pain points for the company.

The business environment today is facing numerous risk like advanced persistent threats that are created by nations instead of individuals which means risk assessments need to be done properly (Cascarino, 2012). New regulations and privacy laws that if broken could create financial hardship or financial ruin for the company. Network perimeters really don't exist, the current company network is composed of nodes in the form of personal computers and smart devices that access company networks from anywhere. In this environment, it's extremely important for companies to react to problems quicker or problems like the Target Corporation will continue to occur. The use of continuous auditing concepts for security is a possible solution. Because auditors are used to creating reports for management and security professionals are used to reacting to security issues. Both sides can collaborate to create quicker reports in a format that management can understand.

Bibliography

Anderson, K. A. (2013, September). Overcoming Barriers Between InfoSec and IT Audit Practitioners. *ISSA Journal*, pp. 22 - 28.

Brisbourne, A. (2014, February 5). *Tesla's Over-the-Air Fix: Best Example Yet of the Internet of Things? .* Retrieved from Wired.Com: http://www.wired.com/2014/02/teslas-air-fix-best-example-yet-internet-things/

Cascarino, R. E. (2012). *Auditor's Guide to IT Auditing.* Hoboken: Wiley & Sons.

Freund, J. (2012, September). A Cooperative Model for Security, Audit and Risk: A Collaborative Approach to Risk-based Audits. *ISSA Journal*, pp. 31 - 35.

Gibbs, N., Jain, D., Joshi, A., Muddamsetti, S., & Singh, S. (2010). *A New Auditors Guide to Planning, Performing, and Presenting IT Audits.* Deloitte.

Handscombe, K. (2007). Continuous Auditing From a Practical Perspective. *Information Systems Control Journal*, pp. 1 - 4.

ISACA. (n.d.). Retrieved from http://www.isaca.org/cobit/pages/default.aspx

ISACA. (2012). *IPv6 Security Audit/Assurance Program.* Rolling Meadows: ISACA.

ISACA. (2014). *A Business Framework for the Governance and Management of Enterprise IT.* ISACA.

Lo, E. C., & Marchand, M. (2004). Security Audit: A Case Study. *IEEE*, 193 - 196.

Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It. (2014, March 13). Retrieved from Bloomberg BusinessWeek: http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data

Ross, S. J. (2012). This Should Not Be Happening. *ISACA JOURNAL*, pp. 1-4.

Sanders, J. (2014, March 19). *ICANN sends registrars and domain owners in a panic*. Retrieved from Tech Republic: http://www.techrepublic.com/article/icann-sends-registrars-and-domain-owners-into-panic-with-2013-raa/

Santos, H., & Pereira, T. S. (2010). A Security Framework for Audit and Manage Information System Security. *IEEE*, 29-32.

Sarva, S. (2006). Continuous Auditing Through Leveraging Technology. *ISACA Journal*, pp. 1 - 4.

US-CERT. (2013, JUNE 14). Retrieved from US-CERT: http://www.us-cert.gov/ncas/alerts/TA13-175A

Ward, M. (2014, Feburary 26). *Energy firm cyber-defence is 'too weak', insurers say.* Retrieved April 1, 2014, from BBC.Com: http://www.bbc.com/news/technology-26358042