Global Information Assurance Certification Paper

Marivic Weiss
SANS GSLC Practical Assignment – Version 1.0

A Security Legacy

Abstract
With the advent of the Personal Computer (PC) and the Internet came the mass exodus from stalwart mainframe legacy systems to the revolution of bringing the power to the user. Technology decision makers were inundated with new applications that were accessible via the browser and marketing campaigns touted how these new products were going to change the way they do business – fast. Departments in an institution or enterprise with their own budgets procured these web savvy products and they started proliferating like mushrooms. And they continue to grow.

Technology has changed so much, but our awareness of how to secure that technology has not followed the same path and in most cases is considered as an afterthought. Often times a very expensive afterthought. Managers were used to the principle that the mainframe legacy systems contained the application and all the enterprise data. The Information Technology (IT) department maintained the administration and performance of the network and these servers. Thus, security is the IT department's responsibility. Right? Wrong.

The legacy of the mainframe era is reflected by current enterprise security awareness. The idea that security software can be procured, installed, configured, and forgotten still lingers. This type of legacy should not endure. Security should be responsibly handled and be on the forefront as businesses move from their legacy networks and systems to web facing servers and applications.

The History

In the past, a line was drawn. Network managers owned the network, system managers owned the computers, programmers created the applications, and on the other side the users were, well – users. Security followed along that demarcation line. Businesses had their own private networks that ran proprietary network protocols that network managers "owned" and secured. The mainframe servers were located in secure computer rooms, ran intrusion detection and auditing software and only the system administrators had the power and the privileges. Applications were installed, customized and maintained by a group of programmers. And the users worked from the green screens on dumb terminals, connected to terminal servers, connected to the server. The IT group owned security and users did not know nor care what security there was. Management was satisfied as long as daily business processes were not impacted.

Businesses were satisfied that they had a security infrastructure in place. The security model of that time was much more simple. The foundation of the infrastructure was the company security policy. Around that foundation vital security requirements were effected. These included non-interference security products such as firewalls, routers, dial-up lines, network monitoring applications that could be implemented transparent to the business process. Authentication and auditing products that could capture user keystrokes provided secure and monitored system access and were utilized to assist in tracking and reporting access violations. Procedural security objects such as a Disaster Recovery Plan, Employee Security Agreement forms were implemented so that matters of security were handled according to best practice standards and procedures.

Security Managers who were usually part of the IT staff were responsible for getting the daily security reports and ensuring that security issues were handled according to company policy and any audit issues raised by auditors were handled and resolved. Security was usually not apportioned it's own budget but included in the IT departments'. Security was not usually at the forefront when an enterprise considered new technologies. Business needs and profit drove the enterprise wheel.

The Internet Evolution

Technological advancements like the Personal Computer (PC), client server computing, relational databases, and the Internet to name a few changed our way of doing business. The PC empowered the user to utilize applications installed in their desktops. The Internet has transformed private networks that were easier to secure to a global interconnected network that continues to grow. Enterprise data is not just located in mainframe computers but in server farms, personal computers on each person's desk, laptop computers, Personal Digital Assistants (PDA), all connected and communicating as part a network of networks. It was a technological revolution unlike any other. The vastness of the network now enabled communication and data transfer through the use of the TCP/IP protocol.

Unfortunately, alongside the Internet evolution in the 1980's, came the hackers, viruses, and various forms of security threats and the security net disappeared. A lot of institutions, governments, enterprises, and consumers did not even realize at times that their security had been compromised. For a time, the hackers seemed free to wreak havoc through any holes they could find. It was not until 1986 when Congress passed the Federal Computer Fraud and Abuse Act could government and industry prosecute individuals who performed these malicious acts.

Enterprises then asked what happened to their security infrastructure. Management called on the IT department and security personnel to reaffirm that they had not been hacked nor were they vulnerable to these threats. Suddenly, Security was at the forefront of their concerns.

A New Security Paradigm

Was this a failure? Should the old security plan be thrown out and start over? The answer would depend on how well the current security infrastructure is performing. The common mistake that enterprises made was to implement a static security infrastructure. Once the security manual was created and implemented, it was placed on a shelf and most often became obsolete because it was never reviewed or updated to mirror the ongoing technology change. When a plan to migrate the system from terminals to workstations was initiated, security should have been planned alongside the implementation path so that they were both in place the day users received their new machines. When a new network component or object is to be introduced into a system, security personnel need to be aware of such an occurrence and the security enterprise model updated.

According to Network Associates, "More Threats + More Devices = More Complexity"[1]. This entails that the new security paradigm should be both robust and dynamic. Robust in the sense that modifications or changes to the technology structure should be covered or introduced into an enterprises' security infrastructure plan and dynamic in that it is continuously being monitored and changed. Since the complexity of the infrastructure is a direct sum of the number of devices or security objects coupled with ongoing security threats the enterprise security solution to balance this equation will reflect the new security paradigm that should be implemented.

The initial goal to change the security model should be security awareness. The whole enterprise should be educated on how a successful attack on their technology infrastructure could affect everyone and not just the IT department. A secure structure could be easily derailed by a call to an HR employee asking for password verification and the hacker successfully getting the information. Security vigilance should traverse the whole enterprise spectrum from top to bottom. Education should be the prime goal of security personnel. It should be realized that their job would be easier if the whole enterprise is aware of, understands, and supports their common goal of securing the enterprise. Management would also realize that security should play a big role in their decision making process as it extends to vendors, customers, and business transactions.

As with any endeavor, it begins with a team. A team for securing the enterprise should exist. This group of individuals should be good representation of the enterprise population and not just "techies". It should have enforcement capabilities and have direct access and support from Management. A typical team might include the CIO, the Information Resources Manager, Information Security Officer, Programs Managers, Data Users, Secretaries, Clerks, Auditors,

[1]Network Associates, McAfee Security, Proactive Threat Protection: Reducing the Window of Vulnerability http://www.mcafeeb2b.com/products/proactive-threat.asp

etc. Sometimes the most inane questions presented will trigger the discovery of a threat.

The team should utilize best practices guidelines in the security industry in the design. The plan should include:

1. Identification and measurement of current and future systems, objects, and business relationships.
2. Security Infrastructure Model
3. Implementation and Customization of the model
4. Education
5. Ongoing test for vulnerabilities (tests should both be internal and from external sources)
6. Post Implementation evaluation
7. Ongoing tracking, update, and maintenance

It will be clear that these steps will be executed continuously to prevent the introduction of unseen security holes. The infrastructure should be able to react to any active threats and at the same time proactively monitor the system to sense the initial stages of any threat. Ongoing user education will be a prime factor to the success of the system. System personnel need to maintain an up to date knowledge of the ever- changing security environment. Auditors will have to be rigorous in scrutinizing the infrastructure.

As the Security market grows so will the number of threats and vulnerabilities to enterprise assets. These companies would not exist but for an ever increasing "need". The model continues to evolve to a very complex one due to technology innovations. The responsibility to secure the enterprise belongs to everyone. We should look at how we secured the old private networks and realize that though the Internet opened our systems to the world, our network still exists. We just have to be continuously vigilant and adaptable to change to maintain an environment that we all feel responsible to secure.

References:

OWASP, The Open Web Application Project, "The Ten Most Critical Web Application Security Vulnerabilities", January 13, 2003. http://unc.dl.sourceforge.net/sourceforge/owasp/OWASPWebApplicationSecurityTopTen-Version1.pdf

Network Associates, McAfee Security, Proactive Threat Protection: Reducing the Window of Vulnerability, 2003 http://www.mcafeeb2b.com/products/proactive-threat.asp (register to download white paper)

Slatalla, Michelle "A Brief History of Hacking", The Learning Channel http://tlc.discovery.com/convergence/hackers/articles/history.html