Global Information Assurance Certification Paper

SANS GSEC PAPER

1/12/2004

Developing and Implementing a Security Plan in a Research/Educational Environment

"There is a new sheriff in town"

Qaadir Haamid
GIAC Security Essentials Certification (GSEC)
Practical Assignment version 1.4b, Option 1

As the story begins, our hero the humble Sheriff (Security Officer) steps into the Saloon (Lab). The music stops, and every cowboy and unsavory outlaw turns towards the door.....

The above scene may seem to be from an old western movie where the sheriff steps into the Saloon to face off with the latest renegade or to relax after a long day at work. However it can also be scene from the life of a security officer at a University or Research Institution. I view these institutions as being similar to towns in the "Wild Wild West" where the laws were few and everyone was seeking to make a name for themselves legally or illegally.

These institutions have many laboratories and offices which are like saloons full of savvy gunfighters or want to be gunfighters who could be your best deputy or worst enemy on any given day. The users or citizens in these towns range from Alice, the Presidents Administrative Assistant, to the Post-doc student or professor who writes his own custom software applications. For instance, Alice decides to download an application that allows her to add smiley faces to her email unaware that the program contains either spy-ware or a Trojan horse. Well then our unsuspecting sheriff could have a big fight on his hands depending on the effects of the Trojan or spy-ware such as Gator.

In education and research institutions a great deal of emphasis is placed on being a pioneer. The researchers, professors, and students pride themselves on developing innovating techniques and technologies. So how do you provide security in an environment where innovations are more emphasized than security? Well how would the sheriff handle the savvy gunfighter who might know a new technique to draw and fire his weapon in three seconds flat? The answer is simple use your brains instead of your gun. If you use your gun you can either get killed or kill someone that might be an asset to you later when you are really getting attacked.

The objective of our Security Response Team is to provide a safe wide-open range or environment where the cows can roam and that everyone can grow and develop. We also have the realistic understanding that sometimes being innovative and being secure can't be achieved at the same time. In such cases it maybe best to make a separate saloon or area for them to roam, that is away from the good townsfolk or in the case of the unruly ones take them to the edge of town and tell them to never to come back. However with understanding and cooperation all parties involved can meet their requirements for a secure good time.

As stated earlier I view these institutions like the "WILD WILD WEST". Wide open spaces with a lot of growth but also the constant potential for danger is always

around the corner or in the next scene. A fertile ground is laid for various network intrusions to be launched from the various wide spread laboratories and offices within these institutions. The majority of the emphasis is placed on network availability and access rather than following a set policy or procedure for secure network computing. It is with this understanding that we decided to approach the challenge of securing our environment from an educational and reforming perspective.

Change is never an easy process however faced with such items as:

- Government Regulations- HIPAA, FERPA Sarbanes Oxley
- Cost of Incident Recovery
- Limited capital resources

  There are several risk areas under HIPAA. Certainly, civil penalties of up to $25,000 per calendar year for each violation are a concern. Severe criminal penalties, however, also can be imposed. These penalties include fines of up to $250,000 and/or up to 10 years imprisonment for inappropriately accessing protected health information for "commercial advantage" or to do malicious harm. [1]

Change can become an alternative treatment to just taking the lame horse out in the pasture and shooting it. In the last decade at most of these institutions the external security measures only entailed having routers with filters and maybe at most a packet filtering firewall. Only within the last few years has the computer security of many organizations been assessed. For instance in the case of three former employees of the Near North Group, an insurance brokerage company, who over a two year period broke into various internal computers to read email and other classified data. The resulting damage, investigation and recovery from this activity were reported by the company to cost approximately $ 645,000 by Fred Foreman, Chairman of Near North National Group (NNNG). [2]

The approach to security and incidents was and still is mainly reactive instead of proactive in the majority of institutions. The advent of the HIPAA has affected us directly since we are a major medical school as well as research facility. The above mentioned items have allowed us to force a change of thinking especially with management who in light of such regulations and incidents has approved the majority of our recommendations for implementation.

The downturn in the economy has also driven more organizations to look at their spending more closely. This has also been helpful for us to push for changes to secure our environment. We have no choice but to acknowledge, that yes we have less money to spend. In all cases looking at the positive, as stated earlier with the cost of recovering from incidents, paying government fines, and losing

research funding have been able to do a comparison of costs for our management. We have shown that the majority of the incidents and regulation violations can be avoided by implementing an overall security policy and plan.

Creating the Environment for Growth

> *"A general dissolution of the principles and manners will more surely overthrow the liberties of America than the whole force of the common enemy.... While the people are virtuous they cannot be subdued; but once they lose their virtue, they will be ready to surrender their liberties to the first external or internal invader.... If virtue and knowledge are diffused among the people, they will never be enslaved. This will be their great security."*
>
> *Samuel Adams* [3]

An environment is not merely made up of internal sources but a combination of external and internal resources combining together to make a whole. The major findings of studies show that having a safe environment whether it is at home, at the playground or at work encourages growth and development. In educational and research institutions this is one of the major goals; to provide a safe and secure playground.

As in the Wild Wild West why would you choose to live in a place that was not safe from outlaws? Why open a hotel or general store when every other month you are getting held up? The cost of doing business is more than just your profit or amount of cash you are bringing in but also how much is going out. In the IT realm, TCO or Total Cost Ownership is seen in the form of hardware and software costs, as well as in the form of downtime due to viruses, hardware/ software failures, and network intrusions.

Our stance has become to be proactive to limit these profit robbers so that worms such as Welchia, MSBlaster and W32SoBig which infected approximately 2,100 of our personal computers, will not place a strain on our financial and manpower resources. We decided to start our process by working on internal and external security separately but simultaneously. The foundation is set by our security policy which is a constant work in progress, especially with the growth of technology within the Information Technology world.

The external portion of our plan we decided to focus on these areas:

- External/ Internal firewalls
- Intrusion detection

- Virus protection
- Border network design

The internal portion of the plan we chose to look at broader topics such as:

- Education
- Policy Implementation/ Enforcement
- Mandatory Anti-Virus
- Authenticated Network Access
- Standardized Desktop
- Centralized Patch Management
- Internal Vulnerability Scanning

Protecting the external access to networks has become a very tedious task. In no particular time or instance are you truly safe if you have a network connection to the Internet. If you just examine the logs from your firewall or IDS, you would likely be alarmed at the constant reconnaissance of your firewall's external access policy. The source of these scans varies from virus/worm infected computers, to competitors, to the seasoned cracker who uses your network to launch an attack on another network. They are assessing our network security so why shouldn't we assess our own network security?

We had to look at what the outside world is seeing when they look at our networks. The first step was to scan our own external configuration which can be time consuming but necessary. We used this information to also verify our external firewall configuration because in large organizations things change so frequently it is hard to keep up. We have found many well meaning Systems Administrators who have changed their servers and moved its IP address but have not updated their records with the security team. We have also found out, in some instances too late, that the new server was not patched or unnecessary vulnerable services were left running.

What also tends to happen in most institutions is that the turnover in IT is high so that the person who installed the firewall box may have left the company years ago. So what you have is usually a systems administrator that they put in charge to change the configuration to add or give systems or servers access to and from

the outside. Akin to on the Wild Wild West were the person with the guns and guts was drafted to be the sheriff. This type of behavior is common at educational institutions and small companies. The biggest question is why do we need a deputy to patrol the edge of town? This question is easily answered the first time that an FBI agent pays management a visit or the institution is held liable for damage caused by a compromised system.

The scanning of the external configuration also gives you a way to audit your firewall policy. We found in our situation that there were many grandfathered servers in the external policy which were no longer in service. This information along with an external policy change log is very useful during an audit by regulators or during litigation that may arise from a security incident. The scanning also allowed us to see the services that are allowed and their versions which allow for tracking systems affected by the latest vulnerability.

Firewalls- External and Internal

So why does a company need a firewall? The reasons given by the SANS Institute are as follows:

Why a Firewall? [4]

- Reduce risks by protecting systems from attempts to exploit vulnerabilities
- Increases privacy makes it harder to gather intelligence about a site
- Enforces an organization's security policies

The firewall is not just having a router that allows certain things and disallows other. The firewall must be able to handle the bandwidth or traffic that will be produced by your organization first and foremost. In our case when we decided to upgrade our existing configuration, we looked for a product that had the following characteristics:

- Capable of handling our bandwidth
- Stable hardware and software platform
- Granularity. Filtering based upon content.
- Well designed logging functionality

The basic types of firewalls are packet filtering, stateful inspection, and proxy applications based. We found that the majority of "packet filtering" firewalls such as Texas A&M 's Drawbridge were only good for basic firewall functionality of just blocking only certain traffic based upon the network and transport layer. However

to get the granularity we needed we chose to look at a stateful inspection firewall so that we could control the filtering based upon content as well.

The choice that we made for our firewall solution has allowed us to grow from a secure network design standpoint. We initially looked at the firewall as a policy enforcement point only, but we have now expanded its use to secure communication with our external affiliate institutions. The previous alternative for us was to have these same affiliates within our network space. This from an administrative and security perspective was quickly becoming a nightmare especially with the latest worm outbreaks.

Virtual Private Networking (VPN)

"Not since the introduction of the Internet has a single technology brought with it so much promise—or so much controversy." (Brenton, 320) [5]

The VPN solution we chose has allowed us to move these affiliates to there own separate networks out side of our firewall. We have implemented the VPN technology to protect traffic or the data affected by government regulations. The other non sensitive traffic is now available to the firewall to filter or discard as necessary. We are no longer forced to disconnect networks at the routers in the case of virus or worm outbreaks. We are now simply able to insert a rule in the firewall policy to drop the traffic and log it.

The VPN, Virtual Private Networking, is the technology of creating an authenticated and encrypted path for data communication has allowed us to interact with our affiliates and remote users in a more secure way. Our satellites offices or institutions no longer have to purchase expensive T1 or ISDN lines but can use local ISP services especially with the improvements in DSL technology. We have implemented simple firewall solutions to protect them from malicious Internet activity and also provide them a safe way to communicate with our laboratories and corporate services. What do you need the Pony Express for when you have Telegraph?

IDS

Our proactive stance has also allowed us to implement intrusion detection technology. However our journey into the realm of IDS/IPS has been very interesting to say the least. We have found that in some cases that a lot of products in this still young and evolving portion of security are a bunch of marketing hype. We decided with the complexity and the rapid development in this area it would be better to take our time and do some thorough research on the products and technology.

The research into IDS/IPS technology has been aided by some really good open source IDS tools. This has also shown to be beneficial for us in the wake of the

recent internet worm outbreaks. We have used our test products to correlate incidents with the firewall logs for incident inception and tracking. The one thing that we are seeing though so far is that the amount of data while being very useful can be overwhelming at first.

The thing that we are seeing with all of our changes or new security implementations is that it will take a lot of resources to use and manage the technology effectively. In the case of IDS the majority of the time will be spent initially not in installation but in tuning the system to your environment. Tuning is basically reducing the false positives that are a given in all computer networks. In Host Based IDS you may see alarms from log files being rotated or in Network Based IDS you may see an alarm from someone querying DNS. All these alarms or anomalies have to be checked and accounted for before you can remove them from your integrity checking algorithm or add them to the database as a known traffic pattern in HIDS and NIDS respectively.

The reason for us wanting to implement Host based IDS was to give our laboratory and department Systems Administrators a tool to monitor the security of their servers and workstations. We chose to provide them with this tool due to fact we were finding during our incident investigations that the time between the initial break in or infection and the discovery of the incident was sometimes months apart. This is true in most institutions such as Universities or colleges where you have remote labs with revolving graduate students acting as the systems administrators.

The product we provided the administrators with takes a baseline of the system in a pristine state, hopefully newly built, and then perform an integrity check on the systems and data files using such variables as write, access, and deletion times as well as many other file properties. In our institution as well as in many like it the key to implementing any tool that will be administered by administrators of varying technical levels is to make using the tool as simple as possible. We have found what may be easy for you maybe difficult or time consuming for someone else to do. In most cases if it is difficult or time consuming then the tool will go unused and the same problems as before will arise.

The Microsoft certification craze placed the emphasis mainly on learning the operating system. The effect of this is showing in the administrators that are being trained not be aware of the security ramifications of placing a new system on the network without shutting down unnecessary services, patching or installing virus protection. We have tried to educate our Systems Administrators, one server or department at a time about the host based IDS tools that we have made available. The results have been positive in the fact the Administrators are watching more closely for changes that happen to their servers, so now we have more deputies to watch the town's shops.

DMZ- Border Network Design

The structure of most educational or research facilities is similar to having a corporation with many different businesses within it. In our case we have a corporate side but we also have the department/ laboratory components. These components vary in size and structure depending on the funding sources that they have available. The funding of these departments also affects the level of priority that is given to computer security. The attitude and the approach of these sections is do we have the money to pay for a full time systems administrator or will we just hire a graduate student to work part-time administering our systems. We have made a major campaign to take the burden off of the departments with less funding by implementing more corporate services to assist them in their efforts.

The major IT services today in most educational institutions are web, email, and multimedia services. We looked at the fact that the majority of the departments were running their own mail and web servers. We view this, being the police of the institution, as a major problem because once again the level of effort to secure and maintain the security on these systems is usually sub-standard. The result of which we have seen in the last few years especially has resulted in an increase of computer intrusions.

We have had the corporate server infrastructure in place for a long time however the accessibility and marketing of these services was not a major priority. Once again in the wake of budget cuts everyone is looking to consolidate or conserve resources. We are using this to our advantage to take over the department's computer resources and place them in a more secure environment like a DMZ. Essentially we are disarming the town's gunslingers because the bullets are getting too costly to buy and the guns too hard to maintain. The design will have the corporate IT section managing and securing the servers but allow the departments or laboratories to still control their content to a certain extent.

DMZ's have become a popular way of offering certain vulnerable services such as web and email which are very susceptible to compromise. We feel by isolating these servers it will allow us to cut down on the internal cross compromises which resulted from compromised servers being used to break into or infect other less secure desktops or workstations. The network design of most of the departments include a file transfer, mail or web server attached to the same sub network as say the patient billing, research data servers and regular desktop computers. The latter would really only need to be accessed for internal business activities while the other servers will need to have external access to and from them.

We are also taking advantage of this network design feature to add services such as wireless, VPN, spam filtering and virus scanning. The design is to have as

much of the traffic that flows from external to internal go through our Demilitarized Zone to be scanned and filtered. The traffic would then be forwarded on to the respective areas of the institution allowing us to cut down on the virus/worm outbreaks, spam email, as well control external network access through dial-up or VPN.

Internal Security

Disarming the town's gunslingers can not be done without their approval and management's approval. What good is a policy if no one knows it exists?

When we began to work on our internal security plan, we realized that the biggest problem we faced was educating our user community and to a certain extent our IT staff.

"What makes a good Security Policy?" [6]

At a minimum a good security policy should be:

- Be readily accessible to all members of the organization
- Define a clear set of security goals
- Accurately define each issue discussed in the policy
- Clearly show the organization's position on each issue
- Describe the justification of the policy regarding each issue
- Spells out the consequences of non compliance with the described policy

These are just a few of the items from the "What Makes a Good Security Usage Policy?" list by Chris Brenton. [6]

Education

I chose these items from the list because of the problems that we faced in developing, implementing and enforcing our Security Policies. As was stated earlier the viewpoint on security at most educational or research institutions is reactive rather than proactive. So everyone wants to play with the latest toys, gadgets or develop their own applications with the only worry being that it works. Our policies have been in place for sometime with constant revision to take into consideration new technology such as peer to peer software.

The big push we have made in the last year has been to educate the user community and enforce our policies. We have begun to get involved in Human

Resources Employee training, EEOC, and HIPAA compliance training. We have also begun doing full investigations into all policy violations. This has resulted in the user community understanding and complying with the policy. The word has slowly gotten out now that violations will result in disciplinary action which in the past we were unable to do due to the lack of concern by the departments, management and the lack of deputies.

The legal department has also been helpful to us by stressing the legal ramifications that can be caused by security policy violations such as file sharing or pornography. These issues can always be stressed from different points of view when trying to get the support of the user community and management. We have seen over the last few months as the users and management have become more aware of the legal and financial ramifications of policy violations the amount of violations have dropped severely. We now do not have to spend so much time with Human Resources or the legal department doing time consuming investigations and interviews.

Anti-Virus

> *A new strain of the ``Sobig'' virus, one of the most virulent e-mail viruses ever, spread quickly worldwide on Tuesday. On Wednesday, it was declared the fastest-spreading virus ever by some experts.*[7]

The increase in virus and worm outbreaks is making us focus on another time consuming task, remediation of virus and worms. After the latest outbreak we sat back and looked at the major problem and why we were having these problems. We decided to look at these areas:

- Out of date OS and application patches
- End of life Operating systems still being used in certain areas
- Non compliance with mandatory Anti-virus software policy
- Email attachment scanning and stripping
- Open Network Access.

All of these items we either have addressed or are currently addressing, but we first decided to focus on the Anti-Virus policy. We have in the last four years implemented a very thorough anti virus landscape. The systems that are within this landscape automatically receive anti-virus updates. We found in the past that the users would load the Anti-Virus software and would never do any updates

which caused us more trouble when the latest exploit or virus was introduced onto our networks.

Authenticated Network Access

The latest worm outbreaks made us realize also that our policy for network access had to be changed. The majority of our infestation began from non institution computers or laptops being attached to our network. We had covered the road into town however the bandits went through the mountain pass to the back side of town. We are in the process of addressing this issue using the feature in most switching networks to force authentication by MAC address. This should also address the issue with system administrators inadvertently attaching new systems to the network without the proper patches only to be infected by Welchia or Blaster within minutes.

We do not address this issue currently in our policy but we are looking at adding it before any physical security changes are made to the network. In cases such as this politics plays a big factor in what you implement now or implement later, but you still have to be aware of the risks that you face. The risks that we see ourselves facing currently because of this problem are as follows:

- Liability issues if software installed on non-institution computers is not licensed;
- Liability and regulatory compliance issues if patient health information and other confidential information is loaded on the computer and the computer is removed;
- Non-institutional computers may not have the appropriate anti-virus software installed, or if installed configured incorrectly, potentially allowing virus/worm infections.

Desktop Standardization

The funding in most education or research institutions is mostly federal, state or private grant money. This instability in funding has caused many of our departments to also cut cost by not upgrading computer systems. This results in having vulnerable Windows for Workgroups and Windows 95 systems still in operation. We did a survey of our computer resources that showed over 39% of our computer systems contained operating systems that will no longer be supported by Microsoft or Apple as of December, 31 2003. This problem has caused our IT staff to spend a lot more time and money in protecting and servicing these systems.

We have begun a marketing campaign to combat this problem which includes providing documentation to senior management about the baseline costs that the institution has incurred in remediation efforts. The standardization of the desktop systems to an operating system and patch level is currently in the process. We found out also in our research that we are spending more money to support these systems than it would cost to upgrade the hardware and operating systems to a standard level.

> *In today's economy and rapidly changing IT landscape, enterprises must measure performance to optimize IT and achieve improved business value.*[8]

Corporations and institutions are moving away from the standard financial budgeting for IT resources. The development life cycle of hardware and software has changed drastically over the last couple of years. This is forcing more institutions to move towards computer resource Life Cycle Management. Lifecycle management is the process whereby computer systems and applications are assigned a certain lifecycle of use, and then upgraded or replaced. The process is usually set up in conjunction with a major software and or hardware vendor to either purchase or lease the computer resources for a standard amount of time. The cost effectiveness of this shows in the form of reduced technical support cost and licensing issues.

We are hoping that by standardizing the majority of the institutions computer resources and implementing a lifecycle management program we will be able to centralize and automate many of the functions such as patching and upgrades. We feel that this will also decrease our time spent in technical support of these systems and allows us to focus more technology advancement and increased service offerings to our user community. We are fighting this battle cautiously taking into account our environment, but as always if change is not done voluntarily, sometimes you force yourself into it by complacency.

Our institution has a very diverse computing environment as do many educational and research institutions. I have tried to outline just of few of the items we are implementing to secure our environment. The fact is that as in the Wild West a lot things are not in your control. However, if you make the best effort to secure the things that you do control, when the unexpected happens you are ready for it. We have made a decision to change from being reactive to being proactive, so we can one day ride into the sunset peacefully.

[1] Clarke, Richard L. **"**HIPAA's Challenge to Finance." **Healthcare Financial Management**.
URL:http://www.findarticles.com/cf_dls/m3257/3_55/71712886/p1/article.jhtml (March 2001)

[2] Foreman, Fred. "Near North Victim of Internal Hacker Group -- Customer Records Secure". 24 June 2002.
URL:http://www.nnng.com/NewsAtNearNorth/press_releases/pr26.html .(10 Dec. 2003)

[3] Adams, Samuel. The Writings of Samuel Adams, ed., Harry Alonzo Cushing G. P. Putman's Sons, 1908, Vol. 4, p. 124.
URL: http://quotes.telemanage.ca/quotes.nsf/quotes/2006c4a887f273188525697c0055be05

[4] Cole, Eric. Fossen, Jason. Northcutt, Stephen. Pomeranz, Hal. SANS Security Essentials with CISSP CBK. USA: SANS PRESS, February 2003, Vol. 1 p.651

[5] Brenton, Chris. Mastering Network Security. Alameda: SYBEX Inc, 1999. p.320

[6] Brenton, Chris. Mastering Network Security. Alameda: SYBEX Inc, 1999. p.31

[7] I searched on Google for "virus outbreaks" 2003 Mercury News. "Viruses should drive sales for Network Associates, analyst says"
http://www.siliconvalley.com/mld/siliconvalley/business/special_packages/security/6586867.htm (21 Aug 2003)

[8] I searched on Google for "TCO Total Cost of Ownership". "Reduce TCO Total Cost of Ownership with Benchmarking & IT Asset Management"
URL:http://www.micromationinc.com/