Global Information Assurance Certification Paper

GSEC Practical Assignment
Version 1.4b
Submitted: October 28, 2003

Presenting Security: A Local Government Case Study

By Nick Batey

Abstract

After I attended the SANS 2003 conference and returned to work, I began reviewing what I had learned and started applying it to a basic network security audit of our county network. Through the course of several weeks, this basic audit quickly turned into many pages of information and consumed many hours of my time. It wasn't long before I realized that I would be asking upper management for a lot of money and more people. Even though the one-time costs are acceptable throughout the year, the human resources and annual maintenance costs are extremely hard to justify in such a tight economy. I didn't want to waste my time with the audit if it would be ignored or passed-off as un-important, so I decided I needed to find out how to present my information to management to maximize the affects.

Using Microsoft PowerPoint, I compiled a presentation to reflect the same format as the audit document and presented it to our internal IT staff as a first step. After receiving feedback on the pros and cons of the initial presentation, I then presented the modified version to some of the other key managers of high security agencies within our administration. After getting more feedback from the second presentation, I presented the information to our county manager. The results of each presentation varied, but our overall security model has been permanently altered anyway.

Section I: The Before Snapshot

In the following sections, you will notice that I have separated the Security Awareness from the Security Concern. I did this because I think both of these are key concepts in all security models and there is a large gap between them where security is often lost.

To me, Security Awareness means that a given person is aware of the potential threats to an organization, but it does not offer any conclusion as to whether that person will alter their actions because of the threats. From my experience, the typical user will ignore known security threats to perform any given action on their computer, regardless if it is work related or not.

The next area, closely related to Security Awareness, is Security Concern. This I define as a person having a interest in the preservation of the security related to a specific set of data. With this, that person would consciously avoid known security threats, even if that means altering the way they do their jobs or avoiding unnecessary actions.

I also think it is prudent to point out that a user without both Security Awareness and Security Concern will still be ineffective in supporting the security of any administration. If we, the computer technicians and leaders, don't educate the users to raise awareness, or the users don't appreciate and apply the education, then the entire process is for naught. The purpose of the presentation is to raise these two concepts to a higher level across the administration.

State of Internal Security Awareness

Within our internal IT department, we would strive for security as a direction. By that, I mean that we always tried to do things in a secure manner and each of us had the responsibility of securing a server or PC when deployed. Unfortunately, each of us also had our own view of what prudent security entails. While we did have several SOPs (Standard Operating Procedures) in place, there were few security standards, checklists, or guidelines for us to refer to when performing a given security task. Each staff member was expected to research the potential threats associated with the task at hand, and use their best judgment on the related security practices. This has the potential to stray far away from prudent security.

The perception of our department was based on the services we provided, not necessarily the security of those services. With other departments asking for new services, and unconcerned or unaware of security, the focus fell on the services rather than security. Because of this, our reputation as an information services department was based on our ability to provide services and not our

ability to secure services. If we failed in our services, it was immediately apparent. If we failed in security, it was virtually unnoticed by the user community without an incident.

Our internal management thought security was delegated, and someone else handled it. They rated our organization as highly secure and, like most internal IT staff members, they liked simple passwords and usability – too many constraints make for too many hurdles to get work done. Fortunately, they also thought we could use improvement in security.

According to our internal programming team, security was considered something the Systems Administrator or Network Administrator handle. The programmers here have never accepted the responsibility for any security within their job function. One programmer told me, "I'll get it to work, you secure it." Another programmer, while implying that nothing will ever happen here, said to me, "Nothing has ever happened here in more than 20 years. Why would anything happen now?"

While our technicians had some security understanding, the technical staff was still lacking in real security knowledge. For example, there were several technical users with administrative accesses to every node on the network, yet had very weak passwords.

State of External Awareness

Management

The overall security awareness for most managers was extremely low. I am unaware of any previous attempts to inform them of any of the security threats concerning their related departments. As well, to my knowledge, there has never been a security education program targeted at raising the awareness of these managers.

We have had an acceptable use policy in place for some time now, thanks to our former technical manager, but due to the legal council it was not as simple as we would have liked. It does state that some actions are not tolerated, but most of these actions are related to abuse of the services we provide – like Internet access.

Several of our managers, and even some high ranking officials, used dial-up services such as BellSouth or AOL and were known to leave these connections open at least 10% of the day while they were away.

Users

Our typical user was unaware of many security concepts. The most we have expected from our users is the understanding that e-mail can contain a virus. Since we have had incidents in the past where a virus has made it into our network and proliferated to some degree, there has been a basic understanding by most users to avoid opening executables from their e-mail. Even though we have been blocking e-mails containing potentially violent extensions, the awareness was there.

From my history of helping users, I have found that many of them share passwords with one another. Sometimes this was for access to data which should have been moved to a place where multiple users could access it. Other times this was just because they didn't *know* another user could access volatile data, or they didn't *care* if another user accessed volatile data.

State of External Security Concern

Management Concern

The managers of our county, as in most administrations, had much more to deal with other than computer security. There were few that pay enough attention to the security needs of the county and even fewer willing to part with precious funding to help provide for it.

External management Security Concern was very similar to that of the general user population. Please read on.

User Concern

As I stated earlier, our users were barely aware of potential virus threats. And even though most users understood that viruses could be contained in programs from e-mail, they would still execute most attachments without hesitation – even if that attachment was nothing more than a joke. The concern our users had for the CIA (Confidentiality, Integrity, or Availability) of their own data was low enough to be considered non-existent.

State of our Network Security Plan

The biggest problem of our security model was resources. We were short in either the money or the man power to accomplish much of what needed to be done on a daily basis to adequately secure the network. To ask for more resources for the sake of security would not have had much more effect than just asking for the resources in general.

During installs, upgrades, or changes, it was our responsibility to know our actions and the consequences of not securing our work adequately. This made security ingrained in all we do; but what level of protection were we to provide? Without standards, checklists, and guidelines in place, there was no way to gauge what we do.

Additionally, our services model maintained that users shouldn't have to be concerned with the technical details of *how* their programs and computers operated. When dealing with information security, users must understand some of the technical concepts in order to understand the consequences of their actions. Most users would never think that their machine could get compromised from a website. Then we asked ourselves, is it reasonable to expect users to keep up-to-date with security when it takes a full time employee to do it for any IT shop? We didn't think it was.

That meant that most of the responsibility fell on the IT Security staff to educate the users and to keep them up-to-date on current concerns and trends. This led to the presentation. How was it most effective to present Security concerns to the user population without them glazing over from the technical details? We would need to keep the users engaged enough to remember the material and apply it, while appealing to their individual losses and gains contained within the actions we need them to perform – or better yet, not to perform.

Section II: The During Snapshot

Following in the footsteps of a security conscious technical manager gave me some leeway I may not have normally had. Most of what I was presenting to our county administration had been previously relayed through him via e-mail or written memo. This gave my recommendations more merit since I was serving as a second opinion.

However, even though these recommendations may have more merit, I needed to build my credibility as well for future security related projects. "If your business credibility isn't established, you will have a tough time building *any* kind of case for projects," Jonathan Feldman, Lessons From the Field: Beyond ROI. If the credibility of my former supervisor, a published technical leader, was not enough to acquire the necessary funds for security concerns, then I had to show how the credibility of the project had the weight to carry itself as well as build my credibility, if I was to accomplish future security goals.

Assessment

I started out considering two different types of audit: Qualitative and Quantitative. A quantitative audit requires a person to address each machine or device on the network and perform an exhaustive audit of every known threat. While this method is extremely complete, it also requires a lot of resources.

The Qualitative audit identifies a subset of threats particularly dangerous to the administration and attempts to identify vulnerabilities by acting through a scenario of each threat. This type of audit is much less extensive on resources, and therefore much more feasible for county government.

I knew I couldn't hope to accomplish an exhaustive quantitative analysis with the limited resources we have here. Using some information I gathered from the CISSP Preparation Guide, I decided to do a qualitative audit and try to address some of the key areas with a quantitative approach. For instance, I audited the firewall as a single machine with every known threat in consideration, while virus protection was handled with several scenarios.

It was very important to understand the difference between qualitative and quantitative audits because I didn't want to mislead anyone into believing that this audit would cover all of our data security concerns, or that by correcting all of the concerns presented would make our data 100% secure. My goal was to establish the need and process for our security foundation. I needed to show that security vulnerabilities warrant a greater level of concern and that every department and individual has an interest in preserving it.

Audit Setup

The format of the audit is extremely important for both the process and the reporting. We modeled our report after our process, since that gave us the most accurate image of what we were able to discern. I think most audits would be formatted in the same manner. Rearranging the information may lead you to drawing conclusions and including information that may not be valid.

Here is a basic outline of how our security audit was formatted:

I. Executive Summary
II. Threats
    a. Viruses/Trojans/Worms
    b. Script Kiddies
    c. Insider or Onsite attack
    d. Hackers
III. Vulnerabilities
    a. Desktop Workstations
    b. Internet
    c. Server Systems
    d. Network Infrastructure
    e. Physical Access
IV. Recommendations
    a. Desktop Workstations
    b. Internet
    c. Server Systems
    d. Network Infrastructure
    e. Physical Access
    f. Enterprise Wide

Collecting Data

As I stated earlier, we are county government. Our budget is always tight, so finding the funds for security auditing software is like telling a good joke … everyone laughs. Because of this, I was limited to several open-source tools: Nessus, Snort and SnortIDS, various password crackers, the dsniff toolkit, several manual tests, and the most important of all … common sense.

I didn't find the open source tools a limiting factor at all. In my opinion, most commercial tools were boasting of features already available in the open source community, but we didn't have to pay for them.

The common sense factor is counted in everything. There are many areas in Information Security where one can just look at a setup and see how it can be improved. If you know that Windows 9x passwords are stored in cleartext, stop ignoring it. Your colleagues are wrong when they say, "No one will ever do something like break into this computer. There is nothing to gain from this machine." One administrative password is all they need for anything they want.

As a last thought, I needed to remember to listen to my co-workers. Some companies will spend thousands of dollars to get consultants to tell them to upgrade their computers for the sake of security, but ignore their co-workers and employees that have been telling them the same thing for years. As you will see in the rest of this document, I failed to follow this rule, and lost a lot of valuable information. Since I didn't believe that others in my department had an interest in security, "I" did this process instead of "us" doing it.

Analysis

Although the audit I performed was basic, I was still able to discover many weaknesses in our systems. While our overall security model was well conceived and implemented, there were areas where improvement was a must.

Since the details of the audit are beyond the scope of this document and can potentially subject us to legal issues or disclosing the very information that I am trying to preserve, I will not go into them. But do note that the audit contained inherent security conflicts that directly affect each department in our administration and there was no way for one department to claim immunity.

Establishing the worth of the recommendations proved to be challenging. "The value of security is easy to generalize but difficult to quantify," (qtd. in Hall 44). To explain how one event that may never happen could shut down the entire administration, seems like a dull sword to upper management. The risk is there, but it's hard to see it in the face of so many other budget constraints, like Cost of Living Allowances.

I thought of trying to show how likely each threat is, but I ran into unnecessary complexity. It's funny how everyone seems to have their own formula for computing this value, when it really seems more like a random number. So many factors are involved in the potential of a given threat, war, macro-economics, micro-economics, mergers, splits, new technology, etc. With so many variables, how could anyone pretend to calculate a hard number to represent this completely?

This was where I decided my credibility really started to matter. As the security leader, it will be my responsibility in the future to know the potential of threats and educate myself on the business impact of each threat. While I can put a percentage on this, it could make the problem seem bigger than it really is or even smaller than it really is. To reduce the amount of time spent on questionable numbers, I think putting a credible face on the technical recommendations gives upper management confidence and accountability enough to accomplish the same goals.

Audience

After I finished obtaining the meat of the presentation, I had to target it correctly. I referred to the "Selling Security to Management" publication by Jeff Hall. In this article, he clearly describes how to utilize several concepts to present your information to virtually any audience.

My potential audience ranged from our internal technical staff, to the external non-technical users. Targeting the relevant information to the correct people required altering the audience a bit to suit the presentation. To this end, I decided to divide the presentation into three parts: a presentation to the IT staff, another presentation to a security team, and a last presentation to the various department heads.

The IT staff was chosen first to ensure that we have a unified team. I wanted the internal department to benefit from the information and provide feedback before I relayed concerns and recommendations to the rest of the administration. I typically try to get as much input from each of my teammates before I recommend any kind of action to the masses. In particular, our CIO needed to be on board. Without proper information, he could not possibly provide the support we needed.

While the IT staff needs no explanation, the security team may. Working with our former technical director, I identified some hurdles I wanted to avoid with this presentation. The most important hurdle related to the path of security information when passed on to our technical director.

As we forward important information to our director, he then filters it and forwards that content on to either other directors, or our county manager. Well, we think a great deal of important security info is being filtered out. While not able to address this problem ourselves without the need of an updated resume, we needed a way to avoid this side effect of our recommendation process. At length, the former technical manager and I thought to form a security team consisting of important departments with a lot to lose from a security breach. The only thing left would be to decide who would be involved.

Deciding who would be involved was fairly simple. There are several high profile and highly secure areas in the county government which need to maintain security and even enhance it where possible. These department representatives should be involved in the initial steps in all stages of the security model. Even if they only relay their concerns and potential loses regarding each stage, their input should be calculated in to make each move especially useful to preserving their security.

Also, this core team would address the security needs as a whole. We decided that we need some outside influence and help to get where we need to go. By raising the awareness to those individuals, we hope to be able to present security ideas and directions as a group of concerned departments, instead of a single IT department. This way, when one recommendation may get filtered by one individual, another may see a benefit and act on it.

Last, we will need to raise the awareness of Department Heads and influential people if we are to interest every department to move in the same direction. This last audience would be the most difficult. Since our image is based on our services, we want the security of the network to be seen as one of our services. It will give our director the ability to then base his direction and projects around proper and prudent security without our department coming under the scrueteny of the administration for exorbent costs.

The Presentations

As I was the one with the mission, I was giving the presentation. At this point, it seemed odd that I was trying to sell security to our internal technical staff. It was then I realized that they all should have been involved from the start. But it was too late for that, so the presentation had to be the starting point.

The presentation to the IT department was scheduled to start at 10:00 am on a Wednesday morning. I decided to go through a final dry run of everything I wanted to cover that morning. Even though I had rehearsed the presentation, I had never really acted it out.

So there I was, in the middle of a conference room giving a presentation to an empty room. At first I felt extremely foolish and began by paying more attention to the door than the content of the presentation. I got used to it over time and many good ideas of how to word phrases, present information, and even the tone of voice I wanted to use for that particular bit started to take form. Even though I spent about 2 hours of the morning doing this, the payoff was well worth it.

The IT Staff Presentation

The IT presentation went really good. I started off with a verbal disclaimer stating, “I know this information is incomplete. Please do not treat this audit as a complete list of our weaknesses, nor the recommendations contained therein to be the answers for all of our known or unknown problems.” I did this in the beginning because I felt that everyone should know how involved this process was. I wanted to make sure that I would minimize those who thought this would handle the security of the county for good.

Next, I went over some details on how this was the beginning of a new security model for the administration. I explained how the information I was presenting was related to tasks which must be performed over and over again – that security is a job, not a one time task, and that this is the start of our ongoing security strategy.

The last thing I needed to cover before I got started was protecting my co-workers and I. You see, we all work in the same department and perform conflicting jobs. The same people responsible for the security of the administration are the same ones responsible for auditing the security. While there were a lot of vulnerabilities found due to the lack of a task being done, it’s not that we didn’t know about it or that we don’t care about our jobs, but that there is a human resource shortage coupled with a lack of concern by those who set our standards. Currently, if we spend our time securing the systems we have in place, while our daily tasks outside of the security realm get neglected, we will likely end up with a reprimand. So I answered the obvious question – why wasn’t this already done?

The rest of the presentation was formatted directly from the audit so it was easy to flow from one topic to the next. The three main topics of: Threats, Vulnerabilities, and Recommendations made for a great division. The information blended from section to section very well.

I was detailing each topic as I went through the presentation. I covered everything from the scanning techniques used to locate vulnerable machines, to the password dumping and cracking techniques sometimes used to gain further access. The whole IT department was very interested and asked a lot of questions along the way, prompting even more details and depth into the presentation.

After an hour and a half, the presentation finally came to an end. There was a lot of interest and it raised awareness significantly. I had half of the department talking of ideas on ways to better security, and snagging me right after the presentation to ask further details on how we can make our security model better.

The Security Team Presentation

I started out using the same introduction as with the IT presentation, but a little less elaborate. Also, since this was the subset of departments I wanted to be included in the security team, I addressed that plan as well, promising more info after the presentation.

The Security Team presentation struggled as it was over technical in a basic sense. I noticed several times that most of the attendees were not very interested in the content being covered and even noticed the legal council falling asleep. From the IT presentation, I knew the information had to be shortened and condensed, and that I did, but not nearly enough. I realized that the technical aspects need to be "converted" into more general terms. Most of the people I work with everyday are very technical, but the people in this meeting just use computers. The technical data I was relaying was just too deep.

The funny part is that I read all about being over technical in security presentations. It seemed as though every security article I read repeated it. However, it is very hard to explain why having a weak password is bad if you can't explain why a particular password is weak.

One thing that did go right … I provided food and drink. I made sure there was plenty of doughnuts and coffee to go around. I know this may seem sad, but even I have been disappointed at several workshops or training seminars that didn't provide anything. It takes so little money and effort, but pays off a lot in the likelihood that attendees will return for another meeting – even one as bad as this one.

The Presentation to Management

This presentation was the best of them all. I went into this meeting with a big concern that I was going to get beat down or belittled by the managers. I expected a lot of skepticism and disdain, but instead I got a very warm welcome.

Using a lot of advice from our technical director, the presentation was completely reformatted. While the presentation for the technical team was trying to relay a mass of information with logical reasoning, I learned from the Security Team Presentation to trim it down to just the recommendations for less technical people. This format was more like a memo. It was a brief explanation that simply stated the top seven recommendations with a one line justification.

The seven items I chose to present were really only on the list for budget reasons. The money was the hard part at this point, and this was the last chance to get it since this year's budget was about to close.

The presentation was given to the department heads during a recurring meeting they attend every week. This meeting, the Manager's Meeting, is headed up by the county manager and focuses on the big picture of needs and concerns of the entire county.

As I went through the list and answered questions, I tried to slip in a few small bits on other security concerns as well. The one that I got across pretty good was a note on using external e-mail programs like Bellsouth, AOL, etc.. This was so effective, that the manager ordered an informative letter to go out to all department heads, educating them on the potential security risks of using these technologies. I don't think I need to point out how well that works for us since one of our security needs is the awareness itself. All we will need to do next is repeat the letter often enough to maintain awareness, but infrequent enough to avoid over saturation.

The biggest item on the list was upgrading all of our workstations to Windows 2000/XP Professional and would cost the county $250,000. On this one, I was met with some questions by the county manager, but none that I couldn't answer quickly. After that, he instructed each department to re-open their budgets and purchase as much as possible towards this goal. The end result of this yielded an additional 310 workstation upgrades.

While we need that money to be put into our budget for future upgrades, this was a major step forward. Getting the county manager to accept security in our future helps the other departments feel more justified in security expenditures; which makes our job to secure the enterprise that much easier.

Overall, the response was astounding. After this meeting, like the IT meeting, I had managers addressing me with ideas and questions on ways to better the security of our administration. That was more interest in computer security than I have ever seen here.

Section III: The After Snapshot

The IT Aftermath

The effect on our IT staff was amazing. One of the big points made in my presentation was the lack of current updates. The CIO was so concerned after the presentation, that he started doing them himself. Even though this was more scary than helpful, the goal was met.

Our internal programming team is now much more security conscious. They now understand that many potential security vulnerabilities are contained in what is programmed in-house, and not necessarily in the Operating System. They now seem to take some responsibility for the security of the administration and I have overheard them talking on the various security measures they could take when implementing some new system. This is a major step forward in securing what we publish both internally to our users, as well as externally to the world.

Our internal password strength is now enforced. We have never been able to enforce this in the past because several of our internal people liked simple passwords. Now, the entire IT staff is required to change their password every 90 days and have at least 8 characters. The user population is a little more complicated without SSO (Single Sign-On), but we will be getting to that within the next year as well.

We are now working on a local security policy as well. This policy is based on our current Acceptable Use Policy and will compliment it to every extent possible. Although, if there is excessive overlap, then the Acceptable Use Policy will be rewritten or simplified.

Security guidelines are now being drafted. This process is taking a considerable amount of time due to the vast array of technology we have in house, but the effort will allow technicians to remove the burden of security trends and focus on the job at hand. While security is a task for all of us, it is the responsibility of the security administrator to address current trends or amendments to the guidelines.

Our infrastructure is being changed and upgraded on an ongoing basis now. We are applying all of the latest versions of software to our switches and routers, while implementing all security measures needed to reach our minimum security guidelines.

Since the presentation, I have also had several IT staff members forward me information on various security measures they have found either on the Internet or in a magazine. For instance, our Assistant Director forwarded an e-mail containing a security white paper. If you remember from before the presentation, internal upper management considered security delegated – someone else handled it. Now, these same people are taking a personal interest in security, i.e. I have successfully raised concern.

The Security Team Aftermath

The security team presentation was a disaster. Not only did I bore the hell out of some of my colleagues, but I am also reluctant to now ask them to join me again for another round in the future. I won't use this as a crutch to not pursue the security team, because I think the idea has merit and I think it will better the organization. Although, I will be changing the format of this meeting to be closer to that of the manager's meeting. If I'm going to expect members to attend, then I better make it more about what their getting, and less about the technical details of TCP/IP.

The Department Head Presentation Aftermath

As I stated earlier, this presentation yielded the most productivity. There is not a lot to talk about here other than that we now have the support of all department heads in security interests. The fact that our county manager showed interest in, and acted on, the security recommendations we presented leads the rest of the managers in the same direction.

One important security landmark in this area regards the accesses to external e-mail systems. After this presentation, and us relaying that we can't provide as many layers of defense against viruses such as BugBear.B when external e-mail is in use, these e-mail systems are used much less frequently. Even though we haven't eradicated them, we are now on the right course to do so.

Another important landmark is funding for Windows 2000/XP Professional distribution. Without presenting the security benefits of such a large volume of purchases to the managers, this would have been purchased over several years. As it stands at the time of this writing, the project is already half way funded and it has only been 1 month.

Lessons Learned

First, fine tune the complexity of future presentations and customize each more acutely. As stated earlier, the complexity of the presentation is the key to

how effective it is. In Jeff Hall's article Selling Security to Management, he explained that the audience should be targeted with the lingo best suited for the attendees. Although this article was very detailed and I could have heeded it more, until you have been in at least one presentation NOT targeted well, you really can't fully understand it. If anyone is doing their first presentation, my advice would be to give it to their non-technical family or friends and try not to lose them while keep them interested … and awake.

After some thought, I think a very basic approach with answers to questions would have been more effective. Saying "There is a problem with X," then answering any questions that may arise with enough depth to draw the non-technical user into more of the gritty details is much better than overwhelming your audience with techno-talk. This includes those things we think are basic. Remember that most people don't understand that their hard drive is NOT their entire PC. Explaining that a problem exists is generally enough to convince most people, while you still have to be prepared to show your work in English when presenting to management.

Next, I found that timing is very important. The presentation should be done at the right time to avoid competition with other things. Since I did our presentation right around budget time, it worked out really well for budget justification, but poorly with time as we needed to continue with the security direction while dealing with last minute budget needs. In the future, I plan to avoid contending with any large county events but also placing the large security purchases near the end of the current budget. This way, there is money to be spent without interfering or competing with other events or purchases.

Of the many valuable practices I learned at the SANS 2003 Conference, the one that stands out the most for me was Defense in Depth. This term stands for a practice of using multiple layers of protection whenever possible, and not being satisfied with a single security control in place – regardless of the effectiveness of that control. Basically, don't put all of your hopes in one protection, have backup protections that serve as multiple layers an intruder must penetrate to compromise the administration.

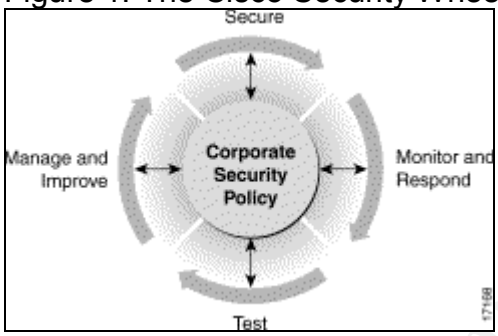
Our inability to procure assets easily makes it more difficult to implement multiple controls for a single threat. In our administration, Defense in Depth is not a very good selling point when recommending a control which does not overlap several other threats. I learned that using one basic control which provided an extra layer of protection from many threats was easier to justify than buying multiple advanced controls for one threat. In other words, by showing how a low cost solution for protection from many threats could be coupled with other low cost solutions to provide a good security model, I was able to purchase more security items to help me reach my goals.

While (THREAT) do { audit; }; done

During the course of this writing, we have gone through several rotations of Cisco's Security Wheel. After monitoring and testing many aspects of security related to our subset of threats, we made security changes to both the network and the policies. Then, we monitored and tested, and made more changes – so on, and so forth.

For those of you not familiar, Cisco's Security Wheel is an accurate depiction of the security process. In the image below, the wheel helps us to see how useful a security policy can be. The major categories of the security process are represented and it all ties back to the security policy. This security policy then acts as a log of the lessons learned over the course of writing it and is an invaluable tool when enforcing good security practices.

Figure 1: The Cisco Security Wheel (Cisco)



The most important implication I see is that there is no way out of this finite state machine – there is always work to be done in security. This is a very important concept to relay to management and this type of information aided me in my presentation to the directors. Showing how a major vendor like Cisco represents security as an ongoing process makes management realize the consistency more than any administrator's words will.

I will close by saying that this report represents more than one **During** and **After** section blended together. By the nature of the security wheel model, this process never ends. It's difficult to show only one rotation of this wheel without including at least some of the previous and next. I think this is a good thing – security is a job, not a task.

Bibliography

Hall, Jeff. “Selling Security to Management” SANS InfoSec Reading Room July, 2001. online. http://www.sans.org/rr/aware/selling_sec.php. (March, 2003).

Cisco Systems Inc. “Design Considerations.” Cisco Press: Documentation July, 2001. http://www.cisco.com/univercd/cc/td/doc/product/iaabu/idpg/design.htm (June, 2003)

Krutz, Ronald L., and Russell Dean Vines. The CISSP Prep Guide: Gold Edition Indiana: Wiley, 2003.

Feldman, Jonathan. “Lessons from the Field: Beyond ROI.” Network Computing Magazine Mar. 2003: 34-41.

Lee, I.. “Presentation Tips for Public Speaking.” A Research Guide for Students July, 2003. http://www.aresearchguide.com/3tips.html. (July, 2003)

Conry-Murray, Andrew. “Justifying Security Spending.” Network Magazine Mar. 2003: 44-49

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event