Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Achieving Executive Buy-in: The Case For Security

Not everyone thinks about security when they should. But with multi-user environments containing business critical data, security is a must. With all the great technology and the magnitude in which businesses and organizations of all sizes rely on information technology, they must also think clearly about security. In most environments network administrators or dedicated security staff have the responsibility of securing these dynamic infrastructures. That being said, many organizations often put security to the way si...

Copyright SANS Institute
Author Retains Full Rights

AD
Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

Achieving Executive Buy-in: The Case For Security

Chad Boeckmann
GSEC Practical Version 1.4b, Option 2
June 11, 2003

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Abstract

Not everyone thinks about security when they should. But with multi-user environments containing business critical data, security is a must. With all the great technology and the magnitude in which businesses and organizations of all sizes rely on information technology, they must also think clearly about security. In most environments network administrators or dedicated security staff have the responsibility of securing these dynamic infrastructures. That being said, many organizations often put security to the way side of higher priority projects or business objectives. This paper conveys a real world approach to selling security to upper management and creating a foundation to build security upon. In order to have a secure infrastructure one must be persistent and creative in making the executives aware of the necessity of having security processes, procedures and standards in place to prevent the organization from feeling the effects of a security breach. User awareness is the key to building a foundation for security and the education must begin with the executives.

Background

I had been an Information Security Analyst for five years when I was hired on with a company I will anonymously refer to as CNE. I was accustomed to working in a mainframe RACF and Unix environment and I had good experience drafting security policies and procedures. When I arrived at CNE to assess their information security situation, I used the defense in depth strategy, but with limited scope. The definition of defense in depth is "the practice of building multiple layers of security into a given system or network. [1]" In most interpretations of this it is pictured like an onion with various layers. Below in Figure 1 is a visual of the defense in depth methodology. I was not granted any special access or authority on the network to perform scans or security testing. Therefore I resulted to the knowledge in which I obtained through conversations with others in the IT department and documents such as outdated logical network maps and organizational charts, which I managed to gather. I just assumed that they really wanted to challenge me. Unfortunately I was not able to thoroughly investigate each instance of the security "onion" in the process which is recommended, from outside to with-in. For the security vulnerabilities I did discover, I followed the 4-step approach outlined below in Figure 2. The process is as methodological as walking down steps. 1st Identify, 2nd Analyze, 3rd Recommend and 4th Implement.

Figure 1

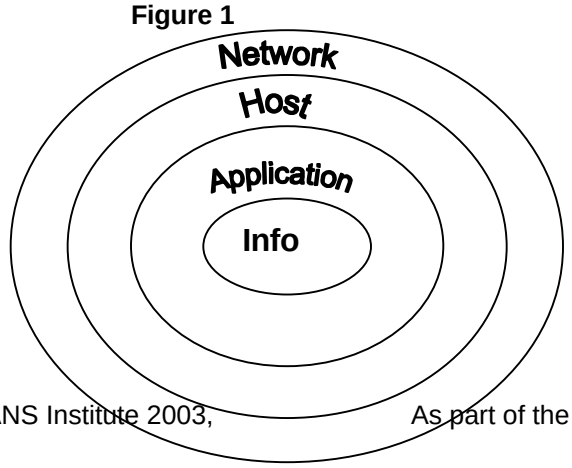
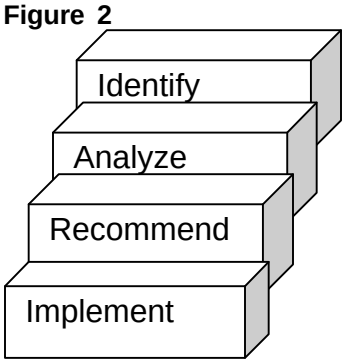


Figure 2



© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Before Snapshot

CNE was formed with the merging of two similar companies. The business merger officially ended in November 2001, which resulted in the newly formed and named organization. When I arrived at CNE in July 2002 they were in the midst of consolidating their information systems. The deadline for this monumental task was November 2002. The companies that existed pre-merger did not have anyone dedicated to the position of Information Security Analyst. I was brought on board to fulfill this role in the newly formed organization.

At the time I had arrived at CNE they had just began a company-wide policy and procedure project. This played a big part in their decision to hire an individual dedicated to the security function. I began my job by familiarizing myself with the IT support personnel and the responsibilities they had. Many who were working towards merging the information systems so their typical job duties had somewhat changed. Getting any sort of buy-in from the IT staff, including management, was tricky. The organization had relied on the trust they put forth in their employees to simulate the assurance that their information infrastructure was secure. The network and database administrators were accustomed to handling security and creating makeshift processes. Many security functions were inconsistent or neglected and standardization was not addressed. My task was to build security initiatives to include new policies, procedures and standards while raising awareness.

Identifying and Analyzing the Insecurities

I had acquainted myself with the infrastructure support group, which was titled 'Technical Services'. This group is responsible for the entire network and the servers on the network. The responsibility fell under one manager. The IT department used the word "security" and communicated to me that they knew the importance of it. I questioned whether they really understood what the term security entailed? My conclusion was "no", they did not. "The term 'information security' means protecting information and information systems from unauthorized access,
use, disclosure, disruption, modification, or destruction in order to provide—

> (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
> (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
> (C) availability, which means ensuring timely and reliable access to and use of information. [2]"

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

I assumed the Technical Services Group was going to be friends or foes of security. As luck would have it, they were friends of the idea of security but foes of having an individual dedicated to such a novel concept. I began my risk assessment of CNE by spending some time with each person in that group to gain a better understanding of what their responsibilities were and how they were carried out. I soon learned that many of the implementations were done in production without being tested first. Also, there was no change log for any modifications they had performed. The majority of the network topology resided in the minds of four key people in that department. If one of those people decided to not go to work anymore, the infrastructure would have been in a state of disarray. I requested from the Technical Services group, any sort of network diagrams that were available. All of the diagrams that I was provided with came with a verbal disclaimer: "these are all outdated by twelve months or more"; but nevertheless the diagrams assisted me in my assessment. It was astonishing to discover that many of the responsibilities the Technical Services Group performed was not documented in any way. CNE also had informal processes for creating new user accounts and resetting passwords. Their security policy was simply an unwritten rule that was assumed to be common knowledge and weak at that. I could see that written policy and procedures was definitely an area that was lacking and needed attention immediately. From the outdated network diagrams and periodic brief meetings, I managed to gain a sufficient understanding of the infrastructure, the business plans and the latest IT projects. There was no concept of project management as the IT department was always in reactive mode. This reactive nature was embedded in CNE's corporate culture. I also paid close attention to other practices, such as the general user community practices. Roughly 95% of the employees in the IT department alone would leave their workstations unlocked while unattended to. I have seen items labeled "for management only" left up on desktops unattended anywhere from 10-45 minutes. It was astonishing to see that programmers, database administrators, technical services personnel and managers were all exposed to the simplest form of a security breach, which I like to refer to as "the lurking eye". I had also witnessed live production code left available to anyone interested. This was my first clue that security in this environment was obscure at best. Below I have constructed a table of security vulnerabilities that I identified and analyzed in my first two months at CNE. Having the items documented and scored assisted me in prioritizing the recommendations, which I developed from the risk analysis outlined below in Table1.

Table 1

IT Resource	Number of Employees Responsible	Major Security Vulnerabilities	Security Rating 1- Good, 2- Fair, 3 – Poor
Internal Network Routers and Switches	2	Either no passwords or one common password is used on these devices	3 – Poor security measures are currently implemented or not used at all.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Firewall	1	Contractor installed and configured this device and no internal employee is well trained to administer this service. One manager is ultimately responsible for the firewall.	2 – It has been configured well to start with but ongoing support is either unreliable and at times support does not exist.
Application Servers	Unknown	The Technical support group would install the hardware and OS but would then release responsibility for the application over to a business group. Many applications could not be identified with a business owner.	3 – No standards in place for application user accounts, passwords and services to various network devices. Application administrators exist throughout the company and are difficult to identify.
Anti-Virus	3, and 1 contractor	The password for the Gateway Anti-Virus has a generic password, the same password used for other administration accounts.	3 – It was a good step to install and properly configure an Anti-Virus solution. However, the password was freely available to anyone with a dictionary. The admin web page could be easily discovered if a user was inside of the network.
Disaster Recovery Plan	1	A plan was written by a vendor and has never been tested.	3 – The manager responsible for the plan stated: "currently the DR plan is to have my resume up to date"
Physical Security System	2	The computer, which had the building security software, installed, was accessible to cleaning staff, receptionists and the office administrators. The program was always logged into and the Pc was always powered up.	3- It is way too easy to add unauthorized people to the building security system. Thus compromising all other security measures to the corporate office. If physical access were gained then information security controls such as passwords and logon credentials would be much easier to discover or bypass.
Change Management	0	Changes to the environment cannot be properly audited or researched.	3 – IT Director stated that this was not necessary and he relied on his managers to project manage and communicate to the department any major changes to the system.
Security Policies, Procedures and Standards	0	Procedures and policies did not exist for the IT department. They relied on the know-how of the individuals in charge of a specific area.	3 – If the individual who was responsible for an IT Resources left the company there would be no document to allow others to perform that duty. No standards in place for user accounts, passwords or common practices.
Workstation Security	Entire Organization	Password protected screensavers were not part of the image used on each machine. Also, no policy to enforce locking the clients when unattended to.	3 – No one even thought twice about locking his or her workstation. This was the most blatant security risk, which the entire company was exposed to.

By having the above vulnerabilities identified I could now begin to communicate to upper management where the most vulnerable areas were and the necessity for having information security built into their business model to help in preventing future security weaknesses.

During Snapshot

It was time to present my findings to management and receive buy-off to begin implementing solutions. I was unsure of the level of security awareness that upper management had, mainly the IT Director and the CIO. With the systems

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

merger in progress, security was definitely off the radar for upper management. The first step was to deliver the basics of information security and explain what information security really means. I did this by describing the three pillars of security: confidentiality, integrity and availability. Another important aspect of educating upper management was describing the reporting structure that security should be under. For security personnel to have influence and more decision making leverage, the security department must report directly to the CIO or in some organizations to the CEO, depending on size and politics. This ensures that security is not forgotten or becomes merely an afterthought. Beginning with the basics was essential to educating and reinforcing proper security practices.

Determining the largest threat

The most difficult task was educating my manager and the IT Director what the term "security" meant and where the biggest threats were, after all there were so many. The toughest part of planning my projects was determining the biggest threat area. Once the assessment had been completed it was clear to me that the largest vulnerability was the end-user community and the network layer services. But I had to focus on one or two vulnerabilities at a time in order to see it through to completion in a timely manner. The mindset of most employees, including upper management was "we sell raw products, who would want to steal that?" If I received a nickel every time someone told me that I would be close to retirement by now. According to the 2002 Computer Crime and Security Survey completed by the Computer Security Institute, "90% of companies and government agencies reported computer security breaches in the past twelve months.[3]" This indeed is a startling statistic. After identifying the insecurities at CNE and doing some research I knew that a security breach on various levels was very likely occurring everyday. Security awareness at the executive level had to come first. After all, they too, are end users and most likely have elevated permissions to the company's data.

Addressing Management

Now that I had identified the major problem areas, it was time to convey these findings to management and receive buy-off to correct the problems. This was another hurdle to jump. When I confronted my manager, an administrative manager, about the security budget for the coming year he stated, "there is no budget". As you can imagine this was a devastating fact. He stated that if projects come up that justify the spending then we can receive approval for such a purchase as long as it is reasonably priced. I then knew that I had to make a very strong case for purchasing any security tools, as this was definitely not a priority for management. It was now my job to make it one. I began by creating recommendations for the security vulnerabilities I had documented in Table 1. Every organization has different office politics that one must live by. I discovered that educating management and users alike about security was the most influential. By doing so, also greatly assists in implementing solutions to the

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

security problems. The approach you choose to communicate the importance of security is going to reflect your success in doing so. In my security briefing with my manager and the IT Director, I presented my findings from the risk assessment and discussed the need to correct the issues. This meeting was well accepted as it gave insight to what the role of a security analyst actually is. Prior to that meeting, my manager and the IT Director thought of a security analyst as one who simply creates policies and procedures but does nothing to enforce them or correct the known vulnerabilities. The outcome was good as I was successful in explaining to them what my job was but at the time no action was to be taken in regards to the security assessment. A large part of this decision was based on the fact that a system merger was taking place and further resources would be unavailable. About three months after my initial meeting with my manager and the IT Director, I called a second meeting to discuss security with the IT Director and the CIO. By moving up the reporting structure to educate about security vulnerabilities and initiatives, it raises awareness of the purpose of security and can help overcome negligence from your peers regarding the issue. Just as I have identified and analyzed the major problem areas pertaining to security practices, I also had to identify the level of security awareness of upper management. I began my meeting by addressing the reporting structure that the security department should utilize by explaining the importance of having a higher level-reporting manager to create further exposure for the purpose of implementing security policy. The response I received was not inspiring. I was told that the reporting structure is fine for now and may be looked at again down the road. At this point my expectations for the meeting were already falling short. Next, I went into the security vulnerabilities I discovered from Table 1 and explained briefly the importance of addressing these known issues. The CIO and IT Director did not want to hear about the problems or even believe that the security vulnerabilities I had identified were issues to be concerned about but nevertheless they asked what it would take to correct the vulnerabilities. My response indicated support from other departments. When I explained the need for policy, procedures and standards the executives acknowledged this as an acceptable task, but addressing the network issues was not an option at that point in time. The reason I was given for this was due to the system merger activities and utilizing other department resources was not an option. If I had been brought on board prior to kick-off of the systems merger, some of the issues could have been resolved prior to creating further changes to the environment. The timing was not ideal but then again, building a security initiative in a new organization does not rely on timing but rather on persistence. The executives viewed the probable solutions to the network vulnerabilities as being one of a hindrance and thus not requiring any action. They also did not want to take on additional initiatives at the time because of the hundreds of activities that were already occurring. Upper management also considered the problems as issues, but nothing that needed any real-time solution. The vulnerabilities were viewed as pre-existing problems and the mentality was that these issues did not stop any business critical processes, at least not yet.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Politics and Policy

Upper management just wanted to know that the issues were being identified and considered. My title was IT Security Analyst, which meant that I had no decision making power or the ability to get tasks completed by other support groups. I felt as if I had reached a dead-end. As time went on, about 3 months, I had discovered various other network security issues as well. My next approach, which in hindsight should have been my first, was to develop policies and procedures to drive the security initiative. "Policy is designed to inform all individuals operating within an organization of how they should behave related to a specific topic, how executive management of an organization feels about that topic, and what specific actions the organization is prepared to take related to that topic. [4]"

Creating policies, procedures and standards assisted in the education and awareness that was needed in order for me to be successful in implementing security in the organization. I was confident that this was the first step I needed to take in order to get any of the outstanding issues resolved. The very first policy that was drafted was the Acceptable Use Policy. The legal department and I had worked together to create the AUP. Thankfully, about the same time I was hired on, the company had initiated a corporate policy project. This was an initiative from their parent company, which was essentially the Board of Directors, to get the policies and procedures in order. By this time I was hired the initial phase of the policy and procedure project was completed. Its objective was to identify possible policies and create a policy and procedure approval process. The Acceptable Use Policy was one of the first policies to be approved and adopted by the organization. To follow-up with the Acceptable Use Policy I created the Password Policy and the Information Security Policy. The Information Security Policy was the justification for everything revolving around information security. The initial draft of the policy was rejected because management stated that half of the policy was not applicable or not in place. I stated to them that having such a policy was the sole reason for getting the things in place to begin with. I had stated that the idea behind the Information Security Policy was so the security issues could be resolved and addressed with policy to back up the actions for doing so. I also advised management not to look at it as a snapshot of today but more like a snapshot of what the IT infrastructure and the corporate culture should look and act like tomorrow in terms of security. At that point I felt as if I was plowing a new road and overturning boulders. The message about security was starting to get through. Management began to understand the concept of security and the rationale that policy does support the actions taken in the name of security. The lesson that I learned was this: sell policy because that sells security.

I conducted further research through various Internet articles and security handbooks and also took into account my past experience to determine the

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

policies and procedures, which are deemed as the most crucial. The most interesting part about my research for policies was that I discovered many public institutions make their security policies and sometimes procedures freely available to anyone. Even for internal processes. Many of these can be used as guidelines for customizing policies and procedures for your environment. A simple search with your favorite search engine should do the trick. The short list I created for my initial policies and procedures are in Table 2 below.

Table 2

Policy, Procedure or Standard Title	Brief Description of the Policy, Procedure or Standard
Acceptable Use Policy	This covered the guidelines and responsibility that users of information resources must follow and be aware of when using any information resource.
Information Security Policy	This included all aspects of information security including, physical security, risk management, database access, end user responsibility and IT specific responsibilities.
Password Policy	States the appropriate use of a password, password guidelines and tips on creating a strong password.
Anti-Virus Policy	Requires the use of an approved anti-virus utility throughout every network server and on each client-side machine. Details the required maintenance of the anti-virus solution.
Security Access Request Process	Details the process and policy for requesting additional security access.
Security Access Termination Process	Outlines the process and policy for requesting the termination of a user account. Also discusses the timeline for doing so and Human Resources responsibilities for notifying of such an occurrence.
Wireless Communication Policy	A policy on appropriate use of Wireless networks, configuration standards and testing requirements for implementing a wireless network.
Standards on User ID Naming Conventions	Details the proper naming convention for user accounts on the various applications and databases.

After having created the Information Security Policy, Acceptable Use Policy, Password Policy, Anti-Virus Policy and Wireless Communication Policy I moved onto the Security Access Request Process and the Security Access Termination Process. I knew that the development of a security request process was going to be the first major project and impact to the user community in regards to information security policy and procedure.

Establishing an Approval Process

I began by interviewing two individuals with little security background who frequently processed security requests. Users through the mainframe email system, which had no way of electronically categorizing the messages, or by fax, routinely submitted the security requests. Each emailed request was then printed off by one of the individuals who had been assigned the task of processing access requests. The printed emails were then filed in a folder and

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

categorized by month and by year. There was literally no way of auditing the access requests without digging through 12 months or more of hardcopy requests and then one could still not be guaranteed to locate the original email. This was a very archaic and inefficient way of producing an audit trail. Another critical attribute of the request process that was missing was the approval process. The general rule of thumb was that a manager could request access to any security screen that he or she felt their employees must have access to, without question. Referring back to what I stated earlier about not following the security "onion", at this point I realized that I must focus my attention at a deeper layer into the security onion; the application layer.
I began to interview a group of people that were in a department called 'User Support'. These individuals were very familiar with the intricacies of the various functions in the mainframe. I began to ask questions like:

1) "What is the most important screen in the Billing menu?"
2) "When the user makes changes in that screen, do the changes occur locally for that user or do the changes occur system wide which affects the data that all users will see?"
3) "Who is generally responsible at the corporate level for the billing data and for customer billing in general?"
4) "How do users generally receive access to this screen?"
5) "Why should there be security on this screen?"

By asking questions formatted in the above examples, I was able to determine the criticality of the access levels each function should be classified as. After repeating this process a couple dozen times I formed a policy and procedure that was titled 'Mainframe Function Approvers Policy and Procedure'. At this point I had enough information from the interviews and organizational charts which I obtained from Human Resources to begin contacting the appropriate business owners for acceptance and approval of the process. I found that when I submitted an email to all of the business owners asking if they are the appropriate person to approve access to a specific screen, they all replied in a timely fashion and appreciated the fact that someone was implementing more control over their area of concern. This new policy and procedure detailed the process to be performed by the security administrator and it identified the business owner assigned to each security function. Prior to granting a user access to specific function identified as "sensitive", the Mainframe Function Approvers Policy and Procedure must be followed. In the policy and procedure was the list of security functions and the respective business owners who must grant approval for each identified function prior to the security administrator authorizing the access. By putting the responsibility on the business owners it accomplished goals in the name of security. The goals obtained were: 1) educating the more influential members of the company the importance of security policies and procedures; 2) requiring those same people to get involved and take responsibility for a small portion of information security in the company;

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

3) raised security awareness for the end users by indirectly informing them that not all security requests will be automatically granted and controls are necessary.

Creating the Security Request Process

An important step in creating the Security Request Process was to require users to request access electronically. By doing so, it established a means to electronically record and archive the security requests. This also assists in performing random auditing of the security levels that each user has. I generated a Microsoft Word request form and created a cover page, which included manager's information and the users information including job title, location, phone number, and employee number. This was the essential information required to properly validate and process a security request. This was also the beginning of a form template that I used for the network services, mainframe security and termination request forms. In the header of my form I wrote a brief summary of the policy and procedure titled 'Security Request Process'. I included in the header the method for requesting access, which stated: "All forms are to be electronically submitted via email to the address: ITsecurity@domain.com." The second item in my summary on the request forms was the general guideline that no one may request access for himself or herself. If users could request access for themselves, it would bypass an initial approval from their department management stating the access is required to perform a job responsibility not to mention it the fact of it being a bad security practice. Lastly, I included the SLA, Service Level Agreement, which I established. Because I would be the only individual to validate requests and process approximately 50% of them which would be mainframe requests, I set the SLA to three business days. I found that this was a fair expectation for both the user community and myself.

After the forms were established, I wanted to have a centralized location for all security requests to be sent to. So I requested a mailbox titled 'IT Security'. Of course I did not have the access myself to create such a mailbox so I had to sell the Technical Services department on the idea and explain to them what the process would be. I had the unanimous vote in getting the mailbox created after I explained that this would save the group time and frustration because I would take the responsibility for validating the requests and verifying the forms were completed and correct. That did the trick. The mailbox for IT Security was created. Now it was just a matter of deploying the form to the local Intranet and communicating to the user community the new process for requesting new, change and removal of security access. On the Intranet page where the forms were placed I included the complete policy and procedure that was titled 'Security Access Request Process'. This described the process for requesting access additions, modifications and terminations. It also described the general guidelines for submitting a request as noted on the request forms themselves. Having important policy repeated in various formats is the easiest way to get the process and policy communicated. This worked well to further inform the users about the policy and procedure by having users read through the policy and

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

procedure before locating the forms at the bottom of the page. It seemed to be effective. I had completed the development and implementation of this process about one month prior to the systems migration date, which made my job of ensuring the integrity, confidentiality and availability of the information and the information users that much easier and efficient.

After Snapshot

With the creation of the Information Security Policy, Acceptable Use Policy, Password Policy, Anti-Virus Policy and Wireless Communication Policy, Security Access Request Process and the Security Access Termination Process, I had laid the groundwork for building more policies and procedures and enforcing the now existing security practices. Implementing security for CNE has been a process of evolution. I had some support indirectly from the Board of Directors by having them initiate the policy and procedure project. This assisted the creation and implementation of the policies and procedures. It also made the policies and procedures easier to accept for the majority of the organization. I sometimes named the audit department and upper management as a reason why the processes must always be followed with few to no exceptions. Doing so took some of the pressure off of myself because it assisted others to understand that there was more than just the security analyst who required that proper practices be adhered to. After all, upper management had accepted and approved all policies and procedures that the organization adopted. This has given me more leverage in enforcing the security initiatives set forth by policy. With the implementation of the Security Request Process, it raised awareness for the user community by requiring them to follow guidelines and making users aware that access levels were being monitored and controlled. Security is now beginning to take a place in an insecure organization. The initiative for security was solely driven by the policy I had established and the few meaningful discussions I had with upper management, who ultimately signed off on the policies. By being persistent and continuing to document security vulnerabilities and writing new policies for management to approve, it assists in changing the corporate culture to becoming security conscious.

Enforcing Security

As of date I am nearing the kickoff for implementing password requirements on the network domain and mainframe environment. We are also implementing a web and email content filtering solution to assist in enforcing the AUP. Having a properly composed and approved Acceptable Use Policy, Password Policy and Information Security Policy greatly assisted in generating these initiatives. It also gives further insight to upper management on the importance of security, what security means, and the array in which it encompasses.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Outstanding Issues

The manager of the Technical Services Group still does not see a real need for the implementation of security tools for vulnerability scanning. The group firmly believes that by doing so will create a “too many cooks in the kitchen” scenario. But with a policy and procedure for risk assessments and incident handling these issues can be resolved. User awareness is also still lacking in the organization. Users are aware of the existence of security in the organization and most understand the importance to have checks and balances. Unfortunately, the majority of the users are still very much in the dark when it comes to day to day security practices such as locking of workstations when unattended to and not sharing user accounts or passwords. With the rollout of a user awareness program many of these issues can be addressed and appropriate practices can be reinforced through education in regards to the Acceptable Use Policy and the Password Policy as well as with the use of security auditing tools.

Conclusion

The systems merger went very well and the security was held in tact simultaneously. Some in management were amazed that implementing, what they thought at the time was just bureaucracy, actually benefited everyone in the end. Security has come a long way in just under twelve months of implementation with limited resources. I discovered for myself that the best security trait is perseverance and determination to get the problems resolved. Even if resistance is felt at the executive level, having approved policies and procedures can assist in conveying the importance of having security initiatives. I have found instances where I could have dropped the problem at hand and no one would have thought differently. Fortunately that has not happened and the entire organization is beginning to see the benefits.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References

[1]Tippett, Peter. "Defense in Breadth." February 2002. URL: http://www.infosecuritymag.com/2002/feb/columns_executive.shtml (May 30, 2003)

[2]Federal Information Security Management Act of 2002 (Title III of E-Gov). H. R. 2458—48, SEC. 301. Information Security. URL:http://csrc.nist.gov/policies/FISMA-final.pdf (June 10,2003)

[3]Computer Security Institute. "2002 Computer Crime and Security Survey." 7 April 2002. URL: http://www.gocsi.com/press/20020407.html (May 20, 2003)

[4]Tudor, Jan Killmeyer. Information Security Architecture: An Integrated Approach to Security in the Organization. *Auerbach Publications*, Florida, 1999: 79.

[5]Walton, Mike, TechRepublic, Inc. "Anti-Virus Policies: Educating Users." 23 April 2002. URL: http://www.zdnet.com.au/itmanager/management/story/0,2000029576,20264777,00.htm (June 10, 2003)

[6]United States General Accounting Office, Accounting and Information Management Division. Information Security Risk Assessment: Practices of Leading Organizations: A supplement to GAO's May 1998 Executive Guide on Information Security Management. November 1999. URL:http://www.gao.gov/special.pubs/ai00033.pdf (May 20, 2003)

[7]Mitnick, Kevin D., Simon, William L., Wozniak, Steve. The Art of Deception: Controlling the Human Element of Security. *Wiley Publishing, Inc*., Indiana, 2002. ISBN: 0-471-23712-4

[8]Krause, M., Tipton, Harold F. Handbook of Information Security Principals, Chapter 1-1-1, Fall 1997. http://www.cccure.org/Documents/HISM/003-006.html#Heading1 (June 10, 2003)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 18th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**