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.

Case Study for Understanding the 30,000 Foot View Before Diving In

Information security personnel have a challenging road to travel. InfoSec folks need to be conversant with a variety of systems, such as: routers, networks, servers, PCs, and applications. We also must be skilled with a myriad of tools, know where to find them, how to use them, how to remediate weaknesses, and still get everything to work. This challenge is formidable, but these items are all technical, which generally may be learned a number of ways, such as through SANS training. This case study addresses the front-e...

Copyright SANS Institute
Author Retains Full Rights

AD

Case Study for Understanding the 30,000 Foot View Before Diving In

Bill Baker

May 15, 2003

GIAC Security Essentials Certification (GSEC) Practical v.1.4b Option 2 Case Study

Abstract

Information security personnel have a challenging road to travel. InfoSec folks need to be conversant with a variety of systems, such as: routers, networks, servers, PCs, and applications. We also must be skilled with a myriad of tools, know where to find them, how to use them, how to remediate weaknesses, and still get everything to work. This challenge is formidable, but these items are all technical, which generally may be learned a number of ways, such as through SANS training.

This case study addresses the front-end soft topics of information security, which may not be so easily learned. The analysis of the business, the security problems encountered, how they affect the business, and their resolution will be covered. To retain some brevity for this paper, the typical technical procedures will be bypassed, as there are many other good sources for these topics. The goal of this paper will be to provide some insight to help the reader become a bit more business-savvy, where gearing solutions to the needs of the organization will help raise acceptance rates.

Setup

Various details about Appliance Heaven have been changed for their protection, but the reader will soon realize the similarities and applicability to many companies. Many of the questions to ask at the 30,000 foot view will be outlined. Commentary will be provided in [brackets] of why these questions are important and how the information could be used or interpreted. Below the questions and commentary will be the answers in { braces } provided for Appliance Heaven's case. These answers will be used to help guide the reader through the thought and resolution process. Some of the questions may seem to be standard, common sense questions, but hopefully, the reader will gain insight into some new ideas, and why they may be pertinent.

A business partner (or partner) will be defined as a separate, independent organization with which the primary company does business. These will be customers and suppliers of goods or services. An example of a customer for Appliance Heaven is Stuff-Mart. This is a retailer which sells appliances for consumers such as you and I. An example of a supplier (vendor) is Transistors-Are-Us, who makes circuit boards for some of the appliances.

Before

Appliance Heaven was a $1.2 Billion U.S.-based manufacturer and distributor of household appliances. They had 17 locations throughout the world, with 10 of those in the U.S. for the 1400 employees. Computer operations were a mix of centralized and decentralized, mostly because of some previous acquisitions.

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

Over time, the management team had come to realize that their business operations had evolved to depend more heavily on computer systems and electronic communication with business partners and customers. They had looked at some of the IT-related problems they had experienced, and determined that they could no longer get by without addressing them. The CIO had hired on slightly under a year before, but had made good headway in identifying the hotspots in IT. She was also a member of the management strategy team, so she'd been involved in discussions of the direction of the business.

The management team had determined they must bring in someone skilled in information security techniques if they were to continue to grow and do business electronically. Sales had been growing, and they had recently acquired smaller competitors and another manufacturer who built products they wanted to add to their stable. As a result, the WAN was growing quickly, and additional locations were being added without knowledge of potential security exposures at those locations. The CIO knew she needed to add someone who could determine the risks these sites posed.

They had had their share of viruses in the previous two years. A few of the employees at Appliance Heaven had inadvertently "shared" viruses with some of the partners. A couple of the viruses, "Love Bug" being one, had forced IT to shut down e-mail for three days to perform cleanup. After the second hit, they realized they did not have sufficient protection in place, lacked procedures to limit exposure during an outbreak, and did not have proper procedures for remediation. A post-mortem on "Love Bug" alone identified that downtime, salaries of affected workers, and the effects of delayed orders cost the company over $150,000. They continually had viruses, such as Klez, draining Help Desk time in trying to keep them at bay. The company website had also been spray-painted in the past. Though IT had been catching and fixing the minor virus outbreaks and the web site graffiti relatively quickly, Appliance Heaven still suffered some embarrassment from their business partners. The CEO determined that steps needed to be taken to avoid outside interface problems like these, which were upsetting their customers.

Some of the business partners had directed Appliance Heaven to their own hosted applications to perform many of the back office functions of component ordering, point-of-sale inventory control, and EDI. A couple of the partners had even placed their own application servers inside the LAN to interface directly with Appliance Heaven's main application system. IT had been given directives by the corresponding VPs to set up connectivity ASAP at the time of the partnership signings. Since there was no one on staff at the time who knew how to analyze the risks of the servers or applications, IT went ahead fulfilling the requests. The CIO and network administrator were apprehensive about connecting to the partners, but didn't know the potential exposures these servers posed.

Many employees had been dialing in remotely to access the internal network systems, such as the ERP and e-mail servers. Some partners were also dialing in to access the ERP system. Phone charges had continued to spiral upward through the years. Now,

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

with more people on the road than ever, the long-distance charges were getting out of control. Overseas travelers were consistently running up huge phone bills, which would show up on all sorts of reports. Managers were constantly being questioned about these charges. From the security aspect, many on the management team had been hearing about break-ins and weaknesses with dialup connections in the news, and had started asking questions. IT could not confirm the present or future integrity of the dial-in method, so it was determined that remote access needed to be addressed. The CIO had recommended looking into a VPN, but needed staff to do so.

Little had been done within the network in the way of security. There were firewalls, but the network administrators had no training on maintaining them. The firewalls had been installed with defaults, ports were opened for many applications without analysis, there were no outbound policy restrictions, and system logs were rarely reviewed. Firewalls and routers at the acquired businesses had not been reviewed before connection to the WAN. It was known that at least one of the businesses had some sort of partner connection. Servers and routers had no consistent policies or configurations, and there were no information system or acceptable use policies in place. Other than the firewall, the Internet access was open, and there had been complaints of some inappropriate material being viewed on some user's screens. The exposure levels were generally thought to be high, and there were known vulnerabilities throughout the network due to the lack of training, documentation, and procedures.

In summary, there were many areas for improvement in security and general IT operations. The items mentioned above were recognized as posing a high risk to the future successful operation of the business. The CIO had worked with the IT staff and management team to raise the awareness of the need for a trained InfoSec person to reduce these risks. The green light was given, and I was brought in to help.

During

When I hired on to help Appliance Heaven create a more secure business, I knew I had a lot of ground to cover in a short amount of time. I was not going to have the luxury of soaking in the environment for six months to be acclimated to how they operated. The first order of business was not going to be technical. It was to find out as much about the business, its people, and its partners as possible, if I was going to successfully implement the eventual solutions. I needed to find out about not only the current structure of the business, but also where it was headed. I needed to identify the people who were going to help get things implemented, both technically and managerially.

I chose to start with the Chief Information Officer (CIO), whom had hired me. Fortunately, she was an active participant on the decision team at Appliance Heaven. I have found that the involvement of the CIO in the direction of the company largely depends upon the individual, the rest of the leadership team, and the corporate culture. Many of the following questions should be asked, but not necessarily asked of the CIO. The individuals to query vary from company to company. For example, in many manufacturing organizations, the CFO may be a better person with whom to discuss

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

these issues. In these companies, the CFO has IT under their jurisdiction, and they are the decision-makers. Following is a list of questions with which I started.

- What is the scope of my responsibility? [Though this had been discussed during the interview process, it always helps to ensure there is a clear understanding of any boundaries one may face. Input from multiple sources should be obtained as a check.]
- What is the scope of the security changes to be made? [Will you be dealing with the corporation as a whole, a particular business unit, or a single server? Identifying the scope is one of the most important steps.]
- Who should be asked for authorization for probes, penetration tests, or enumeration? [ALWAYS ask permission!]
- What is the information to be protected? [Get an overview of the information, where it resides, who uses it, where does it come from, where does it go (i.e. R&D, Marketing, remote location, business partner, etc.)]
    - Who uses the information? [Should be related to above, but you must be clear about each set of information. Its handling may change depending upon the users.]
    - How is the information used? [The response will help dictate how it can be protected.]
- Was the business going to continue to grow as quickly as it had recently? [If growth is going to be high, you need to plan for it. This may require that you change the priority of implementing certain things, such as a DMZ application, if a new location is coming online during the same timeframe.]
    - Through acquisition? [You have considerations of an existing environment to deal with, such as: Potential IP address conflicts, existing firewall(s), routers, routing protocols, server and desktop applications, partner connections, remote access and/or VPN incompatibilities, and corporate culture.]
    - Through building of other facilities? [While this can be a cleaner installation from an infrastructure and security standpoint, the total time required can be greatly increased than that of a conversion. This also affects the implementation priorities.]
    - What timeframes were planned? [If another location were to be acquired or built within the next few months, again, priorities must be adjusted accordingly.]
    - Had any specific locations (i.e. overseas) been determined? [If it were to be an overseas location, connectivity costs and lead times need to be considered.]
    - Who are the contacts at the location? [Always ask for names and contact information when you can. This simple step saves an enormous amount of time in possibly chasing down the wrong person.]
- Are all locations wholly owned by Appliance Heaven? [There are three general levels of ownership. 1) Wholly owned, 2) Subsidiary, and 3) Independently owned. Each of these has their challenges when it comes to decision-making and acceptance.
    - Wholly owned entities generally will take direction from headquarters as they all report to the same balance sheet (accounting source.)

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

- Independents are essentially separate companies that may have been acquired at some point in the past, but for various reasons, have been left to perform by themselves. They generally keep their corporate identities; frequently for brand recognition. They usually only answer to headquarters if they have a losing year, or don't make as much money as they should. They may elect to not accept any recommendations from headquarters.
- Merriam-Webster online defines a subsidiary as: "a company wholly controlled by another" (http://www.m-w.com/cgi-bin/dictionary.) In practice though, subsidiaries land somewhere between wholly owned and independent as it pertains to decision-making and taking direction. Frequently, they tend to operate independently, though they do eventually report to the same balance sheet.
  - Corporate culture, even to the individual location, plays a large part of successful acceptance of solutions. Generally though, acceptance will track along the lines of how the location is owned and supported by headquarters. Wholly owned sites are usually fairly good about accepting direction, as they are tied more tightly to headquarters and decisions throughout the year. They usually enjoy more frequent communication, and one or more senior-level individuals from the location may be involved in the strategies discussed at the corporate level.
  - Subsidiaries usually accept infrastructure and security changes after some discussion and negotiation. If headquarters can show them how they will not add to their workload, how they can improve security, or how they can provide some other functionality not previously available, buy-in can usually be obtained. Gaining acceptance from independents is similar to subsidiaries. Security staff should recognize though, that independent sites may not be obligated to implement your recommendations. This will be largely up to the site relationship with headquarters and your negotiation skills. Note that if you are unable to gain their buy-in, they may need to be handled as an untrusted entity or business partner. There are ramifications for this if they share the same core accounting or inventory systems, though.]

- What is the current company culture like? [This will say a lot about the challenges ahead.]
  - At headquarters? [Gain insight into the local politics.]
  - At other locations in the U.S.? [Helps determine how tightly tied the sites are to headquarters.]
  - At overseas locations? [There may be geo-political issues that arise with overseas locations. Country culture occasionally plays a part in willingness to assist or to accept changes. Language barriers may need to be overcome, as well, which could involve creating a liaison with non-IT personnel.]
- Are there any plans to shed portions of the existing business? [If so, that would raise in priority in order to be ready to disable a large number of accounts or remove the site from the WAN. You also would not want to expend a lot of effort on a location that may not be there soon.]

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

- Ask for an organization chart. [This is always helpful to see who reports to whom. If one does not exist, see if you can have one created by your interviewee or HR. Even unofficial org charts are useful (sometimes, they are even better!)]
- Who are the decision makers in the company? [Continue to break down the decision-making process from the org chart to the actual people. You will need to know, and hopefully create, a good relationship with, each of the people responsible for the areas listed below.]
    - For policies?
    - For IT decisions?
    - For information security?
    - For the WAN(s)?
    - For the LAN(s)?
    - For new applications?
    - For application servers?
    - For the primary application system? (e.g. SAP, JD Edwards, etc.)
    - For doing business with partners?
    - For purchasing?
    - For headquarters?
    - For each location in the U.S.?
    - For overseas locations?
- Who are the project or security sponsors? [These are usually people from the managerial to the executive level, dealing with the business strategy.]
- Who are the project or security enablers? [These may be from business unit directors or department heads, all the way to the system administrators. Relationships and technical credibility will need to be cultivated with these folks. Implementation success is critical at this level.]
- Have there been any IT usage policies in the past? [Without a security policy, organizations may be exposed to the world.]
    - If not, why not?
    - If so, why are they not active now? [The answer to this question may provide insight to potential roadblocks. If the policies languished because they weren't revisited, that's one thing. If an upper-level person killed the policies, this will become part of the equation.]
- What are the general feelings about the use and support of IT among the employees? [Getting an accurate, objective answer to this question will go a long way in policy acceptance. The strategy to use and the expected timeframe to deploy policies may be dependent upon this answer. If the users are open to changes in IT, then a new policy may be introduced at any time without much trouble. If users are frustrated with IT, then any changes related to this area may present increased resistance, affecting implementation schedules and success. A separate directive may even need to be sent involving Legal, HR, and management, or possibly even the CEO. If policies cannot be implemented until the next annual review period, then precious time may be spent waiting for that time to come around.]
- Might there be any IT resistance to implementing any of the coming technical security improvements to the firewall, routers, servers, or applications? [Security staff must always be cognizant of any turf issues within the IT organization. For

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

instance, if the network administrator who had been trying to manage the firewall were to feel I was attacking him, he could be changed from a supporter to an opponent. As a security person, having network admins as adversaries does not make for effective implementations.]

- Are there any individuals, departments, or locations who frequently cause problems with IT decisions? [This is not a nice question, it's highly subjective, and it may not be politically correct, but the astute security person will realize the headache-saving value of having input about this up front. Finding out why these folks are unfriendly to IT may save you months of hassle.]
- What is the budget allotted for improvements? [Can intrusion detection sensors be added to all appropriate locations of your network? Can a tool such as Tripwire be added to your key server(s)? If consultants are needed, is there money available? This will help determine the real scope of what can be done.]
- What is the process for purchase requests? [How long is it going to take to obtain equipment or software, once it is determined? If the procurement process takes 6 days or 60 days, you will need to plan accordingly.]
- What kinds of timeframes are expected for changes to take place? [Reality check to see what are the expectations, and if you will need to work to change them.]

Now that we had covered many of the business-related questions, it was time to move on to the technical arena. Please note that this paper will not address the typical technical analysis of the environment. There are a plethora of resources available outlining procedures for risk assessment for applications, networks, servers, and tools to utilize, etc. The SANS Security Essentials course is a great place to start for all these needs.

To continue this case study as it relates to the business end, the answers received to the above questions are below. The question will be first, followed by the answer from the CIO in { braces. }

- What is the scope of my responsibility? { Corporate-wide, and globally, determine where we are in terms of security, what we need to do, lay out a plan to address the problems, and involve whatever staff you need to implement the changes. }
- What is the scope of the security changes to be made? { We have virus, WAN, partner connection, and firewall problems that we know of. I'm sure you'll find other things in your search, though. Also, you should probably be involved in checking out if a VPN would be appropriate here. Outline all security problems as you find them, and we will prioritize them with the appropriate personnel. We expect you to oversee the changes and implement some fixes that our administrators cannot. This includes the global network. }
- Who should be asked for authorization for probes, penetration tests, or enumeration? { I have the responsibility to keep all systems available. If you can outline what you may be doing, I will check with the appropriate management contacts before you do anything. }
- What is the information to be protected? { The Enterprise Resource System is SAP. It holds the accounting, customer, sales, inventory, and scheduling information. This

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

runs the core of our business. We share this with our partners via dialup and it is only password-protected. We don't want our website defaced again, and don't want to send or receive any more viruses. We have two servers that partners have given us that are currently on our LAN. These servers communicate with the partner locations. Stuff-Mart also has an application server that we access at their location via the Internet. We have sensitive engineering drawings that we ship back and forth between our suppliers and R&D. There are artwork files that are used by Marketing, our graphics department, and a printing partner that show our marketing plans. }

  - Who uses the information? { As stated above. }
  - How is the information used? { As stated above. }

- Was the business going to continue to grow as quickly as it had recently?
  - Through acquisition? { Another acquisition is being planned, but has not yet been announced. The target date is within 90 days. }
  - Through building of other facilities? { One of the U.S. shipping locations is going to double in size later in the year. }
  - What timeframes were planned? { As stated above. }
  - Had any specific locations (i.e. overseas) been determined? { The acquisition is to be in the U.S. }
  - Who are the contacts at the location? { We are getting those, but the people cannot be contacted until the acquisition is complete. Once completed, we will have around 120 days to integrate them into our network and systems. }
- Are all locations wholly owned by Appliance Heaven? { Yes, but we recently acquired a couple of other small companies. We haven't worked with them much other than getting them on the WAN. They are starting to use the SAP system, but still operate their own accounting systems. }
- What is the current company culture like?
  - At headquarters? { People are generally supportive of one another. Everyone realizes we are growing and that changes will be taking place. They don't resist change any more than the normal person. But, if they are informed of why the changes are occurring, things seem to go much more smoothly. The computer skill level of the employees varies quite a bit. Some groups have very savvy computer users, such as Finance. They sometimes want to do things that stretch beyond our resources. We have also had some problems in the past with employees surfing on the 'Net to inappropriate sites and wasting time, though. The management team would like to address that too, if possible. }
  - At other locations in the U.S.? { Each location has its own quirks, but they take direction pretty well from headquarters. Since we own each of the locations, they report directly to us for most major decisions. We have tried to involve their Plant Managers in the strategies for their product lines, so they have time to spread the word at their location for retooling or running another shift. The three companies we recently bought are still operating independently, but we would like to have them adopt the changes we apply here. They have their own IT staff, but we haven't spoken to them much yet. }
  - At overseas locations? { They also are involved in decisions that affect their locations, so they are pretty open to change and direction from here. Their local

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

cultures follow management pretty well, so if management is on board with what we want to do, the changes can usually be implemented easily. }

- Are there any plans to shed portions of the existing business? { No. }
- Ask for an organization chart. { I have the official one, but I will mark it up to show some of the other relationships. }
- Who are the decision makers in the company? { This area is summarized for brevity and to protect Appliance Heaven. In general, the company had a fairly flat structure. The food chain went as follows: Worker/Engineer, Supervisor, Area Director, Business Unit Director, Vice President, CEO. The remote locations had a Plant Manager at the Business Unit Director level. }
  - For policies?
  - For IT decisions?
  - For information security?
  - For the WAN(s)?
  - For the LAN(s)?
  - For new applications?
  - For application servers?
  - For the primary application system?
  - For doing business with partners?
  - For purchasing?
  - For headquarters?
  - For each location in the U.S.?
  - For overseas locations?
- Who are the project or security sponsors? { The entire management team is behind this. They have all realized how much the way we do business has changed over the past few years. They are all willing to do what's necessary to get us where we need to go. }
- Who are the project or security enablers? { The Business Unit Directors are going to be the ones to sign off on any changes. Frankly, they are going to take the recommendations of their own people about technical impacts to their site, though. }
- Have there been any IT usage policies in the past? { No. }
  - If not, why not? {We'd never thought of doing them until you mentioned them in the interview. }
  - If so, why are they not active now?
- What are the general feelings about the use and support of Information Technology (IT) among the employees? { There are a broad range of emotions represented within the company. Some people are still getting comfortable with computers, while some are very computer-literate. There are people in both these skill sets who love IT and some who get frustrated with us. Some of the frustration has been at the slowness that we have upgraded their desktops. Another point of stress is that we have implemented some things without telling them ahead of time. Then it becomes a fire drill to pull in the people to get things accomplished on time. Others have wanted to bring in new applications to help them with a specific function, rather than use SAP's capabilities. In general, people have heard that you are coming, so they know some things are going to change. }

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

- Might there be any IT resistance to implementing any of the coming technical security improvements to the firewall, routers, servers, or applications? { None that I know of. Our network administrator got the firewall thrown at him without any training, so he's glad to get some help with it, if that's the reason for the question. }
- Are there any individuals, departments, or locations who frequently cause problems with IT decisions? { Overall, the users don't complain too much about IT. The R&D department likes to play with things by themselves, and the computer systems are no different. They brought in their own DSL line because we were having some problems with slowness to the Internet last year and they got tired of waiting for it to be straightened out. There is one location which doesn't like change. We always seem to have problems with them. }
- What is the budget allotted for improvements? { Assume that you will have the appropriate funding to get the equipment you need. Just ask first, please. }
- What is the process for purchase requests? { There is an online submission form that gets routed to the appropriate Director. That person reviews the request, adds any comments, and approves or denies the purchase. If approved, the system routes the request to Finance. If Finance blesses it, then their notation is made, and it is forwarded to Purchasing. Purchasing places the orders with our vendors. This process usually takes a few weeks. }
- What kinds of timeframes are expected for changes to take place? { ASAP. It will be up to you to work with myself and the management team to let us know what needs to be done, and how long things may take. }

This was a good first interview. I had continued this process for the first couple of weeks while making other general observations when walking around. As mentioned above, this paper will not go into the technical analysis, but that is exactly where one would want to go from this point. Hopefully, some of the background questions to ask have been outlined, and the reader can see how the solutions may need to be crafted for some of the idiosyncrasies of the organization. The discussion below shows the steps taken from gathering this and the technical information.

Once the information had been gathered during the interview process, the next stage was to perform some verification. "Objective" tools should verify what has been gathered from the interview process. I had asked for access to all the diagrams and documentation that would be relatively current, and asked permission to perform some scans. These scans were planned and executed during authorized windows, and the documentation (that could be found) and information from the interviews was accurate enough to start with. The appropriate people verified, updated, and added to the documentation as it was obtained.

Considering the sizable task ahead, organizing the team was paramount. I put together two teams. I needed to ask for a priority call on the time of the team members, which was granted. The implementation security team consisted of the lead network and system administrators, the lead application developer, and myself. The management security team was comprised of the CIO, a representative from HR, a person from Legal, one of the Vice Presidents who volunteered, and I.

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

Once the teams were in place, the next step was to get some program and issue-specific policies moving. Some samples, guidelines, and procedures were given to the management security team, where HR and Legal worked closely in development. When they had drafts ready, the rest of the management security team would review them and come to consensus on final drafts. These were submitted to HR and Legal for final approval and deployment to the employees.

While the policies were being drafted, the implementation security team started itemizing additional tasks. The initial list went as follows:

- Enumerate all locations
- Review and tighten firewall policies
- Remove "extra" Internet connections
- Make contact and build relationships with acquired businesses
- Review and repair WAN structure
- Review and repair LAN structure
- Determine and implement best remote access method(s)
- Determine better configuration for partner servers and connections
- Review and repair virus protection
- Review primary web site and server
- Implement system standardization and documentation
- Analyze engineering drawings – sensitivity, users, data transfer
- Address large file transfer
- Review SAP access and architecture – methods, users, alternatives
- Set up security training sessions
- Send security memos or newsletter
- Build relationships with IT at headquarters
- Build relationships with IT at remote locations
- Build relationships with management at headquarters
- Build relationships with management at remote locations
- Determine and implement Internet access and surfing policies
- Prepare for coming acquisition
- Determine hardware and software needed to purchase

The list was re-prioritized according to the following criteria:
- Risk factor
- Urgency
- Business impact
- Ease of implementation
- Technical capabilities/Training
- Affected users
- Timing with the applicable policy being implemented
- Timing with other projects
- Partner effects

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

- Staffing/Training
- Project schedules

The implementation security team's suggestions to the management security team were prioritized as follows:

- Build relationships with IT at headquarters
- Build relationships with management at headquarters
- Review and tighten firewall policies
- Review and repair WAN structure
- Review and repair virus protection
- Determine hardware and software needed to purchase
- Determine and implement Internet access and surfing policies
- Review primary web site and server
- Prepare for coming acquisition
- Implement system standardization and documentation
- Review and repair LAN structure
- Remove "extra" Internet connections
- Review SAP access and architecture – methods, users, alternatives
- Analyze engineering drawings – sensitivity, users, data transfer
- Build relationships with IT at remote locations
- Build relationships with management at remote locations
- Enumerate all locations
- Make contact and build relationships with acquired businesses
- Determine and implement best remote access method(s)
- Address large file transfer
- Determine better configuration for partner servers and connections
- Send security memos or newsletter
- Set up security training sessions

The management security team agreed with the priorities, so the presentation of the list was made to the business management team. They initially suggested the web server and determination of hardware and software be moved up in the list. Rationale for the security teams' prioritization was discussed, and they eventually agreed with our recommendations. It was made very clear to all participants that many of these items were going to be "works in progress." For example, changing the firewall was going to be an ongoing process. Many projects can't be performed sequentially, so plan for overlap, but it's best to figure out when those projects need to be started.

Now, a brief background about each item and what was implemented will be given.

- Build relationships with IT at headquarters
- Build relationships with management at headquarters

Sitting down with the people with whom you work and getting to know each other can be not only enjoyable, but is also key to implementing successful solutions. People like to support their friends. If you can successfully build good relationships with your co-

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

workers, you can usually enjoy continued success. As a security person, there are times when you have to draw the line and have a priority call made, but even these instances should be handled with grace. The odds are pretty good that you will have another contact with that individual in the future. Keep in mind that you reap what you sow. Some meetings, which would normally be bypassed, were joined, and I started going out to lunch occasionally with the various players. These relationships helped out very well as things progressed.

- Review and tighten firewall policies

Some low-hanging fruit was selected which would show that progress was being made quickly. Implementing a basic outbound policy on the headquarters firewall was relatively easy, and I had prepared the helpdesk and the implementation team to field any issues surrounding broken applications. I knew the firewalls would be revisited frequently, but I wanted to get started with something that would give us all a little peace of mind. While I was at it, I activated the other LAN port for a DMZ to house externally-facing systems. We would be putting this to use soon.

- Review and repair WAN structure

During the network scans and interviews, I found that the WAN was in need of some attention. There were three locations experiencing sporadic connectivity problems. The WAN needed to behave correctly, as it was determined to move all Internet connectivity to run through headquarters. Once focusing some attention on the problem, it was found the three locations had local network administrators, and they were not running the proper routing protocols. I took the opportunity to start building relationships with them, and to inform them of upcoming security plans. Throughout the WAN, there were multiple sites with Internet access. The team was not prepared to unhook them on the initial go-around, but identified the equipment at the site and worked with the local network admins to get some basic firewall policies in place temporarily.

- Review and repair virus protection

Viruses had been a continual problem for Appliance Heaven. Fortunately, all e-mail flowed in and out through the servers at headquarters, and not through any of the other Internet connections. Even the acquired companies had their MX records pointing to headquarters. There was virus scanning on all desktops, but updates were user-initiated. The first thing the team did was to get virus scanning on the mail gateway and post offices. Next, we configured another low-use server as an update server. This server was configured to automatically go to the vendor site daily for new signature files. (Yes, we had another firewall rule change for this.) The administrators then pushed down a desktop configuration change to automatically pull signature files from the update server weekly and run full scans daily.

The incident handling procedures were reviewed and enhanced. Procedures were put in place to monitor the virus scan vendor's web site daily for news of major outbreaks. When those occurred, the mail logs were watched more carefully for traffic anomalies. During more serious outbreaks, a blanket e-mail was sent out to the users to caution them to watch out for symptoms of the virus. We exploited those events to serve as

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

user training. Scaled procedures for remediation were written should an infection occur on a desktop or server. These procedures were tested on a lab server and were put into action on the desktops occasionally.

- Determine hardware and software needed to purchase

The team had put the review for hardware and software as the next priority, but in actuality, this was going to need to be revisited frequently. I had tried to condense this step to a particular point in time, but the best that could be done was make an estimate to management of the budgetary numbers for hardware and software for security-related items. Some of the items included in this analysis were: anti-virus server software, a VPN package, proxy servers, FTP server, a couple of other servers, and additional telco circuits.

- Determine and implement Internet access and surfing policies

Internet access was to going to need to be approached like eating an elephant, one bite at a time. It would take a while to shed the extra connections throughout the WAN, so it was approached in phases. The first phase was to do a quick review of the firewall policies at the site and tighten up the rules until we could get to phase two. Eliminating an Internet connection is always a sensitive issue with the site personnel. Once the Internet Usage Policy had been implemented, the admins were able to set up redundant Linux proxies with Secure Computing's SmartFilter software to control access to web sites. We also set up a server to spool log files, which started with these proxy logs. The log server would be utilized more often as the security infrastructure was built. Once the core surfing systems were in place, the users and locations could be moved over to access through the protected systems at headquarters. Routing changes were implemented at the location when it was time to migrate. Then the admins were able to push down browser changes to reroute users through the proxies. I did meet quite a bit of resistance at one of the remote sites, though. Through my earlier questioning, it sounded like there might be some problems, so I was prepared. I had an "unofficial" org chart and learned that the transportation manager had influence over many of the locations, including this one. I had built a good relationship with him by spending some time to install and train him on a personal firewall for his laptop. I had a conversation with him, he in turn had a discussion with the folks at the location, and the migration continued.

- Review primary web site and server

The Appliance Heaven web server had been installed with nearly all defaults, and I found it had actually been compromised multiple times. Working with the lead developer and one of the server admins, we temporarily moved the site to a spare server. We took the original server offline, wiped it completely, then loaded and hardened the O/S. Lastly, we configured the Apache web instance in a more secure fashion, loaded the content back on the system, and put it back into service on the new DMZ. Procedures to keep the O/S and Apache up-to-date were implemented.

- Prepare for coming acquisition

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

Regarding the upcoming business acquisition, it ended up being pushed back another 90 days, which was just as well. Dealing with it right up front while the implementations were just starting was not the best situation. Eventually, the other company was bought out, and they were able to be quickly assimilated into the Appliance Heaven environment, including the WAN, e-mail, and Internet connectivity. A couple of site migrations did need to be pushed back when the sale was finalized.

- Implement system standardization and documentation

Standardizing routers and servers was going to be a long process. As long as a lot of the systems would be touched in the coming months, it was felt the groundwork should be laid for standardization. The new servers implemented would be templated for the appropriate O/S. If an existing server was to be reworked, the goal would be to get it as close to the template as possible. Documentation of systems needed to be done, even though we knew it would slow us down in the interim. The log server was utilized as the TFTP server, since it had more than enough horsepower, and it was protected pretty well.

- Review and repair LAN structure

The LAN needed a lot of work on the security side. While it was operating fairly well from a network perspective, there were few controls in place to guard and monitor key systems. The detail with this item is much too voluminous to cover in this paper. Suffice it to say that the process of segmenting the network in a different fashion began. Password policies were addressed on all systems, personnel with administrator rights were reviewed and reduced, and intrusion detection was put in place. The log server was widely used in this phase.

- Remove “extra” Internet connections

Removal of the extra Internet connections was discussed above. One additional point worth noting is the preparation that occurred between headquarters and the site personnel. I didn’t call up one day and tell them their Internet connection was going away. I chose to work from the top down on this one. The management security team contacted the Plant Managers and outlined the follow-up to the policy deployment. When the circuit removal was presented as a cost-saving measure (which it also was), the Plant Managers readily accepted the transition. There was much less resistance taking this approach. People are generally apprehensive about having something taken away. If the issue can be presented in a positive light, it is usually more acceptable.

- Review SAP access and architecture – methods, users, alternatives

The SAP system was going to need an improvement plan all its own. This was an important item, but it had been lowered in priority as a new module was being implemented first. Employees and partners alike were accessing this system. There were controls within the application for the information that could be seen, but the network access was wide open. Remote employees and partners were dialing into a modem pool to gain entry. Eventually, I re-architected SAP, and the web access portion of SAP was installed on a separate server, which was placed on the DMZ. The application and database servers were left on the LAN and network access to the

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

servers was trimmed. The partners were moved to access SAP only via the Internet and the account rights were reviewed. Once the VPN was set up (which will be outlined shortly), the remote employees were migrated over. They could still access via the web, but found the VPN access to better meet their needs.

- Analyze engineering drawings – sensitivity, users, data transfer

Engineering drawings were found to be the heart and soul of Appliance Heaven. Should those have fallen into the wrong hands, confidentiality would have been compromised. I had found that these large drawings had been scuttled around the world via e-mail. Not only were some of the partners on dialup complaining, since they'd receive huge attachments, but the integrity of the development had been at risk. There were no change controls on the drawings, so it had happened that development of components was running on the wrong iteration of a drawing. I wasn't going to tackle the change control problem, but a poor-man's solution was to put up a hardened, named FTP server on the DMZ. The team weighed the risks of hosting the FTP server versus outsourcing, and determined that hosting was a good first step. We wanted the server to be fully under our control during the mindset change from using e-mail to FTP. We structured the server to be the central repository for the shared drawings. These would be posted in encrypted form, and each partner and user was to use a secure FTP client, which we sent with some instructions. This allowed the remote sites to download the drawings at their discretion, rather than have them forced down via e-mail polling. Also, the drawings and transmission were encrypted, which was a notable security improvement over clear text e-mail. The team eventually revisited the hosting question and decided to leave the server on the DMZ.

- Build relationships with IT at remote locations
- Build relationships with management at remote locations

I had started building relationships with the remote locations almost from the start. The team had put the starting priority of these lower, but as the occasions arose to discuss the configuration of the sites, I took the opportunities to get to know the folks.

- Enumerate all locations

The remote sites were enumerated over an extended period. Usually, when anyone on the team entered into a discussion about a configuration or the site had some problem, the opportunity was taken to run some tools to verify their layout. Permission was asked from both our management as well as from the site folks.

- Make contact and build relationships with acquired businesses

The acquired businesses were relatively open to changes that were suggested. There was no more resistance than the original Appliance Heaven locations, except for one site. That site needed to be reassured that we weren't coming in to chop heads. After we outlined our plans and how the site personnel were to fit in, we had much more success with our implementation. During the interview with the CIO, I had found out that this site was wholly owned. They were being folded into the corporate structure, but our

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

implementation team happened to be the first corporate representatives to make changes other than WAN access.

- Determine and implement best remote access method(s)

Upgrading the remote access method was a large project. Eventually, it took over a year to complete, but it was well worth it. Not only had the dial password policy left something to be desired, but the long distance and circuit costs were substantial, as well. It was decided to supplant the dialup method with an Internet-based VPN. The vendor was selected and the hardware implemented. Once tested, the rollout started with the sales folks and other employees who regularly dialed up. Out of this batch, the people who had the highest telco charges were migrated first to help with the return on investment (ROI.) The savings realized with the top fifty users nearly paid for the whole project. By combining the IP access controls of the VPN device with the previous LAN resegmentation, I could now control to the IP address where in the network remote users could travel.

- Address large file transfer

There were other large files moving inside and outside the organization than just the engineering drawings. The graphics department regularly generated artwork that was used for marketing or ad campaigns with the customers. E-mail had previously been used, but had not been the right tool. These types of files were migrated to the secured FTP server and the guidelines given to all the partners working with the graphics and marketing departments.

- Determine better configuration for partner servers and connections

The partner servers given to Appliance Heaven had been residing on the LAN. The partners had modems on their servers to perform remote upgrades and maintenance. Operationally, the data flow was from the core SAP system to the partner servers, which did some intermediate processing, and batch communication at the end of the day to the partner site. The port openings and process flow were evaluated, and it was determined these servers could be placed on the DMZ to get them off the LAN. Firewall rules were changed accordingly. The modems needed to be left on, as the partners didn't have any other maintenance options.

- Send security memos or newsletter

It was nearly a year until I got to a point of being able to send out a formal security newsletter. At the outset, employees were inundated with security information from the policies being implemented. We used the serious virus cautions to raise the level of awareness, as well. Since some security information was already in front of the employees on a regular basis, I didn't want to add any more. I started slow with the newsletter, running it quarterly, with only a couple of articles. I wanted to keep it small, knowing people would just pitch it without reading if it got too long.

- Set up security training sessions

Both the implementation and management security teams discussed holding security training sessions, but the consensus was to bypass this formal effort. I was able to give

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

short presentations during company meetings at headquarters. I visited some of the remote locations as part of the analysis and when changes were being made, held some ad hoc sessions for IT and management. I had actually done some training right up front for the implementation security team to get them familiar with the principles of information security. The rest was on the job training.

After

Starting at the 30,000 foot view was extremely helpful in quickly getting a feel for the organization. It also provided a mechanism to quickly identify the company hot spots and scope the path ahead. While the CIO had identified many of the issues from an overall perspective, she didn't know the depth of some of the problems that an InfoSec person would recognize.

While security is an ongoing process, not a destination, the security and management teams felt we had brought Appliance Heaven up to an acceptable level of protection in the year and a half I was there. Let's take a snapshot and summarize the results:

- Company-wide program policies were implemented. There were some issue- and system-specific policies put in along the way, but we first needed to start with the general program policies. Once the policies were formalized, distributed, and signed off by the employees, we could move forward with the security enhancements.
- Relationships had been built and nurtured to help win acceptance of many of the changes put in place. This included management and administrators, as all would be involved in some form or another.
- The LAN resegmentation helped build a more secure structure upon which we could build. Coupled with the WAN, DMZ, and VPN changes, controls were now in place to more securely guide users within the LAN. Also, employees were now the only users on the LAN.
- The risks posed by the WAN were addressed by mapping out each location, tightening up existing firewall and routing policies in the first pass, and analyzing other external connections. The remote site Internet connections and firewalls had eventually been removed, and the sites had been routed through the headquarters proxies for surfing. There was still a fair amount of work yet to be done at each site after the initial phases, such as finding alternatives for the partner connections and standardizing systems, and these would continue for some time.
- Viruses were no longer as much of a threat as they once had been. The vulnerabilities of the gateway and post offices had been reduced by putting virus-scanning software on them. The automated update and scan procedures implemented on the desktops kept things reasonably up to date. Users were still users, and an occasional virus would slip in, but the measures developed to eradicate a virus were effective in limiting the exposure of the partners and the rest of the company. There had been another serious virus outbreak on the Internet, but the controls installed effectively protected the company now.

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

- The web site hardening was successful, and placing the server on the DMZ with proper firewall rules, logging, and maintenance procedures, helped us sleep.
- The partner servers, which had been moved from the LAN to the DMZ, were operating fine, firewall ACLs to allow only approved traffic, and having the partners off the LAN helped put our minds at ease.
- Deploying the VPN was one of the most successful projects accomplished. The risk of war dialers and weak passwords was greatly reduced, as the number of active modems was trimmed substantially. The remote users could now be controlled by group and IP address as to the systems they could access. Inexpensive Internet connections could be utilized with encrypted communication. The resulting ROI left management scratching their heads as to why they didn't do this project sooner.
- The primary firewall at headquarters had had a facelift. Outbound policies were installed, a DMZ had been created and effectively used to get externally-facing systems off the LAN, and inbound policies were reviewed and became much, much tighter. Procedures and training were implemented to review port-opening requests when new applications or servers would come into the picture. The logs were spooled to the log server where scripts could scan for interesting traffic.
- Server and router standardization was under way, and would serve to ease the support burden when building new systems, and in the event of a component or system failure. These steps had already helped to bring an application server back online more quickly when it suffered a drive crash.
- The addition and movement of the web access portion of SAP to the DMZ helped get the partners off the LAN. Access rights were reviewed and updated within SAP. There were ongoing improvements that would need to be made, but changing the architecture was a good first step.
- Setting up the FTP server on the DMZ enhanced the confidentiality, integrity, and availability of large files being shipped around the world. These sensitive files were now encrypted and the start of version control was introduced.

The management team and employees around the world were all affected by the changes to some degree. Throughout the process, people learned that protecting corporate assets was everyone's responsibility. The level of awareness of this responsibility had been raised, and Appliance Heaven has gone on to grow more securely.

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

References

Bayne, James. "An Overview of Threat and Risk Assessment", 22 January, 2002.
URL: http://www.sans.org/rr/audit/overview.php (11 April, 2003).

Merriam-Webster.
URL: http://www.m-w.com/cgi-bin/dictionary

Cole, Eric, et al. SANS Security Essentials. Reading: SANS, 2002.
Section 2.2, pg 5.

Northcutt, Steven et al. SANS Security Essentials. Reading: SANS, 2002.
Section 2.1, pg 3.

Swanson, Marianne. "Security Self-Assessment Guide for Information Technology Systems" November, 2001.
URL: http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf 29 March, 2003.

Davidson, Mary Ann. "With Security, You Get What You Pay For", 14 March, 2002.
URL: http://zdnet.com.com/2100-1107-859767.html (15 April, 2003).

Hulme, George V. "The Threat from Inside", 10 April, 2003.
URL: http://www.informationweek.com/story/IWK20030410S0009 (15 April, 2003).

Secure Computing's SmartFilter
URL: http://www.securecomputing.com/index.cfm?skey=85 (16 April, 2003).

Tripwire's Tripwire for Servers
URL: http://www.tripwire.com/products/servers/ (18 April, 2003)

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

Last Updated: May 24th, 2013

Upcoming SANS Training

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

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
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
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 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 San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	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 Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced