Global Information Assurance Certification Paper

Help we just fired our only IT person!
Doug Cox
November 7, 2002

Abstract

You are sitting at your desk when the call comes in from a business acquaintance asking for help because they just fired their only IT person “for very good cause”. As you ask questions, you realize that your acquaintance has a real problem. You find out that there is no documentation, no knowledge of passwords, critical applications are exposed to the Internet, users are unhappy and they don't know where to start. Your business has provide services to them before and writing a new contract is not an issue. How do you start?

Once onsite, you try to get a snapshot of the situation at a high level. Sit down with the contact and work through the issues to get a deeper understanding of the hot buttons. Look for their immediate exposures, develop an understanding of the corporate culture, map out a plan of attack and start securing the infrastructure. Some things should be obvious like changing passwords. Others are a little more obscure, like finding hidden remote access servers. You will uncover many other problems as you go, so keep your eyes open. Some will need immediate attention and others will take longer. This study covers about 18 months of activity at the pace that could be absorbed by the organization. It is not meant to be universal solution, but lessons taken from a real event.

Before

To hide the name of the health services provider that this paper is about, it will be referred to as the “Organization.” The consulting group that helped solve its security needs will be referred to as the “Group.” The Group has been supplying non-computer clinical services to the Organization for some time.

The Organization is not a technically savvy concern, focusing on the well being of people, very few of their processes were automated. However, when a request to spend over $50,000 came to the CFO for the purchase, installation and necessary training for a CheckPoint Firewall product, suspicions were aroused. Was there enough vulnerability and liability to necessitate a solution costing $50,000? The previous project to stabilize their Internet connection had been a disaster and had caused more issues than were solved. The culture of the Organization was not to place great importance on the information technology infrastructure. But when this infrastructure did not perform to expectations complaints were lodged to the CEO.

The Organization dismissed their in-house computer person. This person had spent most of his time working on starting his own company and had marginally addressed the needs of the Organization. Previous support had been provided by a small retail systems integrator, who was more interested in having

a client that would pay for his test bed than providing real support. The CEO of the Organization requested that the Group formalize an arrangement with the Organization to assist with their Information Technology (IT) development plans and to help them meet regulations such as Health Insurance Portability and Accountability Act (HIPAA). The contract was signed.

The plan of attack was broken down into several steps. These included preventing any retaliatory action on the part of the dismissed employee, stabilizing the infrastructure, upgrading the accounting system, replacing the payroll / time & attendance system, stabilize the e-mail system and web strategy, and position the Organization to acquire a new patient records system.

When the Group entered the picture the Organization was outsourcing its Web Hosting and Internet E-mail to a small ISP located in Florida. The Head of Development set up this arrangement prior to the CFOs arrival and had purchased the ".com" and ".org" domain names. The following systems were up and running: Novell server for the clinical system and three NT servers for proxy, communication, file / print, and e-mail. The network was a mixture of 10baseT and 100baseT all with category 5 wiring. There were several machines with modems for various reasons (payroll, supply ordering etc.) There were approximately 50 workstations on the network with six network printers at the Home Office. Office One had one workstation with a dial-up connection. Office Two had an ISDN line for network connectivity and a small server providing print services, with the remnants of a Cytrix installation, and four workstations. It was a confusing set up that had a lot of history, but had never reached full functionality.

Occurrences of prolonged outages of Internet services, workstations locking up or crashing, and the accounting system freezing were increasing the frustration level of the department heads. Each department controlled their operation including some of the technology assets. There was no formal control or policy with regards to hardware or software. This produced a very unstable network and finger pointing was rampant. Being sensitive to the organizational behavior was very important. The CFO who had responsibility for the Finance & Billing areas was appointed the contact for the Groups efforts. Development, Human Resources, Volunteers, and other business units used the connectivity, file services, web and e-mail but ran no multi-user or server based applications like Finance & Billing.

To date, most of the equipment had come from various donations of either equipment or cash to purchase specific items. Most of the hardware was several generations old and operating systems and application versions were all over the map (processors as old as 486s and Windows 95 to 2000). Some areas had "experts" make small Access Database Applications or Excel macros for small tasks, often loading unlicensed and incompatible versions of software. In the past, the internal support person, if one existed, was called upon to support these applications as well as the sanctioned ones.

There were no formal written policies or procedures for the Information Technology part of the business. There were no acceptable use policies, guidelines for equipment or applications. Very few of the machines had virus checkers; those that did were out of date. IT was not part of corporate thinking and thus was not well managed. But the importance of a stable IT environment was becoming very clear.

During

The individuals directly involved from the Group are Doug and Kevin. From the Organization the CFO, Jan, is the point of contact and the person responsible for the information systems. Kevin's area of expertise is Windows and Novell and Doug's is networking, unix/Linux, and Windows. Doug took on the leadership role and Kevin provided input. Using the principals of Confidentiality Integrity and Availability (CIA) we prioritized the immediate threats and vulnerabilities. The first priority was to secure the physical and electronic assets from any retaliation by the dismissed employee. The next step was to perform an audit of the current environment. At that point, we developed tactical and strategic plans to fulfill the business requirements and institute a security program based on the Confidentiality, Integrity and Availability (CIA) triad. Using Risk as a classification of acceptability (High being not acceptable and Low being acceptable), Vulnerability as the exposure, issue, or target of attack, Threat as the likelihood or possibility of the vulnerability, and Value of the exposed asset, we developed a Risk Matrix for the Organization.

Before Risk Matrix

Risk	Vulnerability / Issue	Threat	Value
High	Retaliation	High	High
Medium	Non controlled Internet access (i.e. Auto answer modems on network workstations)	Low	Medium
High	Mis-configured servers, software, applications	High	High
High	Un-patched software	High	High
Medium	Shared passwords	Medium	Medium
Medium	Sketchy internet connection	Low	Medium
High	Server crashing / locking up (data loss)	High	High
High	No defined server back-up procedures	Medium	High
Medium	No written acceptable use policies	Medium	Medium
High	Servers exposed to the Internet	High	High
Medium	Remote locations uncontrolled	High	Low
Medium	No understanding of the physical topology	Medium	Medium
Medium	Power issues	Low	High
Medium	Workstations freezing or crashing	Low	High
High	Virus	High	High
High	e-mail	High	High
Medium	Web	Medium	Medium
Medium	Rouge applications	Medium	Medium
High	Domain name ownership issues	Medium	High

Step one – secure the asset!

The CFO, who is a trained CPA, did not have a full understanding of the infrastructure. The Admin or root password was not available. To secure the asset it was deemed appropriate to change all passwords and disable any account that was not recognized. Starting with the Novell server running Netware 3.11, Kevin used setpwd.nlm to reset the administrator password. This system has very few users and all passwords were reset. The NT servers had their Administrator password reset using "bd010114.bin". User accounts were either locked or had their passwords reset. Employees that had there passwords reset were notified to see the CFO for a new password. Next, we examined the former employee's workstation and found that it had dial-in access server enabled and evidence that would support the claim of inappropriate behavior. That machine was disconnected from the network and phone lines. Then the hard disk was imaged using Norton Ghost. At this point we felt that our goal of protecting the assets from remote exploit were reasonably accomplished. The lock on the server room door was changed to prevent physical access. Employees, especially on the lower levels, were notified not to give access and report immediately the presence of the former employee. It was felt that these were reasonable precautions for physical on-site protection.

The other two locations were notified that the former employee was no longer with the Organization and not to give him access. The equipment at these sites were used as stand alone work stations and were in need of updating and virus protection. For the immediate task they were not considered significant risks at this time.

The next asset to secure was the ".com" and ".org" Domain Names of the Organization. While the Administrative and Billing contacts also needed to be updated, the former employee has put his name as the Technical contact on the "WHOIS" record. Straightening out this record was a muti-step process. The ".com" was registered as an individual and the ".org" was registered as a business. The employee who registered them was now consulting with the Organization and was willing to help transfer the ownership of both Domains to the Organization. Our first attempt to have the assignments changed was to have this person submit the request using her e-mail account as the authorizing mechanism. This person was willing to help out but did not understand the process, so it failed to change. This was also during a period when Verisign was undergoing process changes. Finally, after several calls to their 800 number, we determined that we had two processes to follow because one Domain was registered as a business and one as an individual. Verisign's phone support has improved drastically and we now have a correct "WHOIS" record.

Now that the primary threat was mitigated we moved on to step two, the implementation of a security program. Being a small organization with a very informal corporate culture, the idea of a heavy handed IT policy was not going to be accepted. The strategy was to slowly implement a computer use/security

policy that would meet minimum principals of the CIA. First verbal policy then written documentation. The initial step was to implement password requirements, i.e. assign each user a password, forbid the practice of sharing passwords, set a minimum password length, and enforce saving confidential files on the server in protected folders.

The server room contained four servers. The Novell server running a business system that was at the end of its life cycle, with vendor support to stop within the next 18 months. The Novell application required a fat client on the workstation and was used only by the billing department. This was the most secure and stable system the Organization possessed. To secure customer data on this platform each user was asked to change their password, unused accounts were removed and the Novell client was removed from those workstations not needing access.

The remaining three servers were Windows NT4 machines and upon examination it was determined that no maintenance had been done for some time and several updates needed to be applied. Server One was setup as a proxy firewall, network back-up, and dhcp server. Server Two had communication applications: Cytrix server, Remote Access Server (RAS), and modem sharing server. Server Three provided e-mail using MS Exchange and, file and print services. There were questions about versions and licenses for each of these services. The Organization was more than willing to purchase the necessary licenses and media for those applications that were actively being used and supported the mission.

The goal was not to take functionality away, but to straighten out the mess with as little disruption as possible. Realizing that communication with the users was absolutely paramount, each user was surveyed as to how they used the system. This was very enlightening, as it became evident that the users did not know the technical names of the applications they used but referred to them by the person who set them up or the business function it performed. With this knowledge we decided to approach the removal of services with recovery and restoration as the primary goal. A service was shut off, then a waiting period of five days for confirmation that business functions were indeed not disrupted, next the service was taken off line and finally removed, if possible.

The first server to be addressed was Server Two. We could find no evidence that the Cytrix server was being used, either locally or remotely. This service was disabled. The RAS and modem sharing services showed no activity in the logs. These services were also disabled. After waiting a week this machine was powered down and after two months was removed from the network to be redeployed.

Server One was looked at next. The proxy server also showed no evidence of use as the Internet service had been switched from ISDN to ISDL provided by Verio and the ISDL/ISDN Netopia Interface was providing network

address translation (NAT) services. The proxy service was disabled. However, dhcp services were being provided by this server. This service was left running until another dhcp server could be established at which time it was disabled. Additionally, the network backup application was hosted on this machine.

Server Three provided the greatest challenge. There were a few "executives" that wanted to continue to use the exchange server and since the Organization was able to find a license for 10 seats it was determined to let these few continue to use Exchange in a limited manner. Additionally, access to the Exchange server was only allowed from inside the firewall, all internet mail when out via smtp to the e-mail provider. The print services were handling those few printers that did not have their own dedicated print server, either HP jet direct or Netgear. Upon examination of the file system, it was very evident that employees who had left the Organization were still active on the system and their replacements were using the old sign-ins.

Only current employee's accounts were left enabled. All other accounts were disabled. This was done with advance notice that the system was being worked on and if there was problems accessing their files to please call the IT phone number to have it resolved. We did not tell them exactly what we were doing but let them know if they had problems how to get them resolved. This revealed that most of the data files were being accessed with old sign-ins. The files were transferred to the correct owner. Next, the system was backed up twice, the backups tested, inactive accounts disabled, and their associated files deleted.

This clean up procedure greatly helped the accounting application by eliminating freezes caused by disk space depletion. This step alone allevated much fear and frustration as the users could stop worrying about data loss.

The accounting system's developer had announced a major release of the software. The plan was to order a new server that would could be partitioned and support the business needs of the Organization. As applications and business units were moved on to this platform, groups would be set up and security measures implemented.

On the two remaining NT servers (Server Two and Server Three) F-Prot Antivirus™ from Frisk Software International was installed and registered so virus definitions notifications would be sent to the administrator. The availability, functionality, and pricing structure was very attractive to the non-profit Organization. F-Prot was also installed on the workstations as will be indicated latter. Again the servers were backed up and now the recommended Service Packs were installed on the NT servers.

A backup policy was implemented that stated:

- Servers shall have a full back up at the end of each week (Friday after close of business) and differential backups Monday through Thursday.

- The system shall also be backed up on a new tape at the close of business each 15th of the month and end of month. That tape shall be taken off site and stored for accounting purposes for seven years by the CFO.
- The backup process is to be tested and verified on a monthly basis.
- The backup log is to be checked daily by the system administrator.
- There shall be three sets of tapes current, one generation back and two generations back. Each set shall be replaced the first of each year.

At this point the servers were felt to be reasonably secure and stable. Confidentiality was enforced by username, password, and groups. Each employee was educated about the importance of keeping passwords secure and not sharing them. Integrity was increased by the removal of unneeded services and hardware. And availability was increased by stabilization of the servers through applying service packs, removing users who were not needed, freeing up disk space, and increasing RAM memory if slots were open.

The workstations provided an interesting challenge. Our goal for this step was to understand the network layout and the condition of the workstations. Starting after close of business on a Friday night we set about to map, inventory and clean up the workstations by cleaning the registry, deleting temp files, scanning disks and defragmenting the file systems. The dismissed employee had stated that the network wiring was a mess and that the labels were meaningless. This turned out not to be true. Every labeled jack had a corresponding jack in the communications closet. We mapped over 80% of the network on to a set of floor plans. There were one or two without labels that were easily identified and labeled. Overall, the accountability of the wiring was excellent.

We looked for a freeware tool similar to the personal inventory client from BelArc Advisor, but did not find one in a timely manner. Our goal was three-fold 1) evaluate machines for upgrade or replacement, 2) inventory applications for license issues, 3) perform system maintenance (i.e. Reg Clean, Scan disk and defragment). Machines that could not run the current business software were pulled off the network. There were several machines that were given memory upgrades to make them useful. All machines left on the network had their operating and MS Office product updated. Additionally, the workstation version of F-Prot AntiVirus™ was installed and set up to have the virus definition updates pushed from the local server during login. There were a few viruses found during this activity and they were removed. A determination of license requirements was made. If there was a business reason for the software to be on a particular workstation a license was verified or purchased. If there was not a business need for the software it was removed. All workstations with modems were verified to have dial-in access disabled. No supported application required that feature.

New machines were ordered for the Home Office and Office Two that had

dial-up connectivity. To facilitate support, security and usability, Doug convinced the Organization to develop a standard hardware configuration and software image for all new machines. This image was also used whenever an existing machine needed to be reconfigured. This base image consisted of Windows 2000, StarOffice 5.2, Power Archive, F-Prot and Reg Clean. MS Office, Adobe Illustrator, Adobe Photo Shop were added for users that had a business need, versions and licenses were controlled. Other software was added upon request and licenses tracked.

There were many complaints about the availability of the network, both internal and Internet. Upon examination it was determined that the communications closet did not have a UPS supply for the ISDL /ISDN router or the network hubs. Power to this location was adequate but not stable. Small power fluctuations were a frequent occurrence. The addition of the UPS solved this issue.

While the above was being accomplished, a network strategy was being implemented. Given the uncertainty of the broadband providers in the area, it was decided that each site would have a firewall box that then connected to a ISDN or DLS router. This would allow for minimal disruption in the event of a change in provider or connection type. Using three of the machines that were removed from desktop service, Doug built three identical RedHat 6.2 systems. The boxes were configured with minimal services. All services were denied except sshd and smtp on the external interface. This was accomplished using tcp wrappers (hosts.allow and hosts.deny) and adopting the ipchains firewall script by Robert Ziegler in Linux Firewalls. On the internal interface dhcpd, caching DNS, and Network Address Translation (NAT) services were provided. Initially, users would have unrestricted out bound access to the Internet. The ipchains rules logs all events and LogWatch reports daily activity. Verification of open ports is monitored with nmap.

Also, a Virtual Private Network (VPN) was set up between the offices. Initially, a product called Tunnel Vision from Canada was implemented between the three offices. This allowed the remote offices to print to the Home Office and the Home Office to print to the remote offices. In addition, the remote offices now had access to the the Organizations file servers, although performance was slow. If this proved to be of significant value to the Organization, a faster connection could be purchased.

The Tunnel Vision product was unable to handle the routing of two remote offices and the Home Office. Another VPN product was selected, VTun and was configured as described in LINUX VPNs. Doug set up an Intranet using 10.0.100.0/24, 10.0.200.0.24 and 10.0.300/24 address space. The caching DNS and NAT were then added at this time to the firewalls and disabled on the other devices.

When the new server arrived, a Dell Dimension 4400, it was upgraded to 2 GB memory, four 18 GB drives were added to the RAID Controller, virus

protection installed, and service packs were applied to the Windows 2000 server operating system. The financial application was migrated over to the new server and only the accounting application users were given access to the application. After three weeks of running on the new system the accounting application was upgraded with no space depletion incident. The new server also handled the new Payroll / Time and Attendance provided by Ceridian. Other groups will be migrated to the new server but only allowed access to their department's area controlled by their access rights, providing separation of services over the next nine months.

Web and e-mail services are currently outsourced to a Web hosting company which has been a moderate success. Aside from some billing issues, they have been happy with this arrangement and feel that there is little risk in allowing an outside company to handle these services. As the user machines were stabilized and other efforts were made to make the system and network more robust, complaints about the e-mail system subsided. Each user is responsible for POPing their mail and the system is configured to store the mail folder on the network drive which is backed up as described earlier.

After

The Organization's IT system security is greatly improved. However, maintaining this improvement is an ongoing process. Going from an uncontrolled, un-maintained network is a step forward in security. However, this is not a final solution and requires monitoring. The concepts of “Defense in Depth” and CIA are implemented. The Organization is growing and changing. This will force the IT infrastructure to adopt to these changes to keep the network secure.

The high risk issues were addressed immediately and others took time to implement. This case covers a period of 18 months. Some issues went away. Others were just mitigated. New issues will need to be addressed. Security is not a static thing, it requires ongoing vigilance and effort. The problems presented here are not unique but are very real.

Mitigation Matrix

Vulnerability / Issue	Mitigation procedure
Retaliation	Has been mitigated by awareness application and network configuration.
Non controlled Internet access (i.e. Auto answer modems on network workstations)	Modems have been verified as disabled for auto answer service. The machines are monitored for changes and new modems. Most rooms have a digital phone lines making it difficult for modems to be added.
Mis-configured servers, software, applications	Have been configured correctly and monitored.
Un-patched software	All software that required patching has been patched.
Shared passwords	Policy is in process of being formalized, employees have been educated and informed.

Remote locations uncontrolled	The Home Office IT person monitors and supports the remote locations and the firewalls are monitored remotely
No understanding of the physical topology	Network is mapped on the floor plans of the building.
Power issues	UPSs were put on all critical components, power is now stable.
Workstations freezing or crashing	This situation has been corrected and they are monitored for free space. Virus detection is updated regularly and standard image is in use.
Viruses	Virus scanners installed on all machines and have regular maintenance
e-mail	Still outsourced and considered a low risk. Users are happier now that the network is stable and there are fewer outages.
Web	Still outsourced, considered a low risk. The feeling is that they do not have the expertise or resources in house to manage correctly. Better relationship with provider.
Rouge applications	Better controlled but still an issue.
Domain name ownership issues	Organization now has ownership and control of ".com" and ".org"
User Education	A new concern that will need to be addressed.

References

SANS 2002 Annual Conference. Security Essentials. Orlando, FL. April 1-7, 2002.

Last Updated: April 23rd, 2018

Upcoming Training

Mentor Session - AW SEC401	Detroit, MI	May 01, 2018 - May 17, 2018	Mentor
SANS Security West 2018	San Diego, CA	May 11, 2018 - May 18, 2018	Live Event
SANS Northern VA Reston Spring 2018	Reston, VA	May 20, 2018 - May 25, 2018	Live Event
SANS Atlanta 2018	Atlanta, GA	May 29, 2018 - Jun 03, 2018	Live Event
Community SANS Bethesda SEC401	Bethesda, MD	Jun 04, 2018 - Jun 09, 2018	Community SANS
SANS London June 2018	London, United Kingdom	Jun 04, 2018 - Jun 12, 2018	Live Event
SANS Rocky Mountain 2018	Denver, CO	Jun 04, 2018 - Jun 09, 2018	Live Event
Community SANS New York SEC401	New York, NY	Jun 04, 2018 - Jun 09, 2018	Community SANS
SANS Crystal City 2018	Arlington, VA	Jun 18, 2018 - Jun 23, 2018	Live Event
SANS Cyber Defence Japan 2018	Tokyo, Japan	Jun 18, 2018 - Jun 30, 2018	Live Event
SANS Oslo June 2018	Oslo, Norway	Jun 18, 2018 - Jun 23, 2018	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 18, 2018 - Jun 23, 2018	Community SANS
Community SANS Madison SEC401	Madison, WI	Jun 18, 2018 - Jun 23, 2018	Community SANS
SANS Minneapolis 2018	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	Live Event
Minneapolis 2018 - SEC401: Security Essentials Bootcamp Style	Minneapolis, MN	Jun 25, 2018 - Jun 30, 2018	vLive
Community SANS Nashville SEC401	Nashville, TN	Jun 25, 2018 - Jun 30, 2018	Community SANS
SANS Cyber Defence Canberra 2018	Canberra, Australia	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS Vancouver 2018	Vancouver, BC	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, United Kingdom	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Charlotte 2018	Charlotte, NC	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, Singapore	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DC	Jul 14, 2018 - Jul 21, 2018	Live Event
SANS Malaysia 2018	Kuala Lumpur, Malaysia	Jul 16, 2018 - Jul 21, 2018	Live Event
SANSFIRE 2018 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 16, 2018 - Jul 21, 2018	vLive
Mentor Session - SEC401	Jacksonville, FL	Jul 17, 2018 - Aug 28, 2018	Mentor
Community SANS Bethesda SEC401	Bethesda, MD	Jul 23, 2018 - Jul 28, 2018	Community SANS
SANS Pittsburgh 2018	Pittsburgh, PA	Jul 30, 2018 - Aug 04, 2018	Live Event
SANS August Sydney 2018	Sydney, Australia	Aug 06, 2018 - Aug 25, 2018	Live Event
SANS San Antonio 2018	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, India	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS Boston Summer 2018	Boston, MA	Aug 06, 2018 - Aug 11, 2018	Live Event