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 - TruSecure Security Certification

This paper describes the security certification process conducted by TruSecure Security Corporation on a company called K-Co; this is a fictitious name used to protect the innocence of the financial firm used in this case study. We will start out by analyzing K-Co's current security position, then discuss financial benefits that can be realized by certifying a company's security program. Following this we will discuss the company that was chosen (TruSecure) based on their certification program and the types of security...

Copyright SANS Institute
Author Retains Full Rights

AD

Case Study - TruSecure Security Certification
(Why Not Certify The Company)
GSEC Practical Assignment Version 1.4b
Option-2 Case Study
David Vos
01/24/03

Abstract/Summary
This paper describes the security certification process conducted by TruSecure Security Corporation on a company called K-Co; this is a fictitious name used to protect the innocence of the financial firm used in this case study. We will start out by analyzing K-Co's current security position, then discuss financial benefits that can be realized by certifying a company's security program. Following this we will discuss the company that was chosen (TruSecure) based on their certification program and the types of security services it provides.

The case study will then outline the actual test steps performed during the certification process. Details about vulnerabilities that were discovered will be discussed, including mitigation efforts to close and prevent the vulnerabilities from further threat. Examples covered in this case study span both logical and physical sides of security including types of hardware and techniques used during each scheduled test. Recommendations will be outlined as vulnerabilities are discussed, including a final recommendation on how K-Co can mitigate future risk on its own. It cannot be stressed enough how important it is to ensure that a company is certified in some fashion when it comes to security. There are many security certification programs; while some are better than others, they all enhance security to a certain degree.

Before: Analysis/Situation of Certification Process
This case study follows a Security Manager, who we will refer to as Bill and the processes he undertook to certify K-Co security processes. Bill was responsible for obtaining a security certification program and attaining a certification by year-end 2002. He works for a financial firm called K-Co that acts as a custodian for individual retirement accounts. Financial industries provide considerable potential risk; therefore, this was a high priority and time-consuming task for Bill and his employees. Fortunately, K-Co is large enough to support its own Security Department. Not all companies have this luxury, which provides more reason why they should look into a security certification program. One needs to remember that the status or size of a company is no barrier to hackers, viruses and other security threats. While K-Co has worked diligently to increase its security presence, it lacked the understanding and manpower to monitor and conduct penetration assessments on its network. These tests are beneficial to assessing the strength of systems on its network and discovering where possible vulnerabilities may reside; thus K-Co had to make a decision immediately.

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

The Security Manager started out by analyzing K-Co to discern the company's current position with regard to risk. Bill created a brief overview of the current security architecture for an understanding of what tools were currently in use and what security functionality was provided. The Security Manager measured risk by considering the threats to K-Co; such threats included hackers, viruses, physical security, improperly trained employees, disgruntled employees, contractors, modems, default installs and authentication. He also noted areas that lacked security mechanisms, including intrusion detection, virus scanners, network scanners, database scanners and policies. These provided Bill the ability to understand potential vulnerabilities and where potential threat could be manifested. K-Co did deploy certain security devices to assist in hardening its network. A BorderWare Firewall for Internet connectivity and a CheckPoint Firewall for web presence was already in place. In addition intrusion detection systems were deployed inside and outside the firewall. StealthWatch, an anomaly-based intrusion detection system, filtered traffic outside the firewall, while NetProwler, a signature-based intrusion detection system, monitored internal traffic coming from K-Co's firewall. This approach provides security for known attacks, as well as unknown attacks discovered by the baseline security and distinguished by the anomalous intrusion detection system. K-Co also deployed a three-tiered anti-virus structure that will be discussed in further detail later in the paper. After Bill was able to quantify the risk according to what was at stake among his vital corporate assets, he started looking for the right security certification program to meet his department's needs and the needs of K-Co. After gathering this information Bill compared different certification programs and identified the best-of-the-breed to certify the security at K-Co.

Certification Process - Analyzing TruSecure's Abilities & Benefits

The company chosen to certify K-Co was at the time called ICSA (Information Certified Security Associates) Labs, which is now an independent division of TruSecure Corporation offering testing and certification of security products. For the purpose of this paper, ICSA is referred to as "TruSecure" even for background information. TruSecure is one of the leading security certification firms and has been helping secure organizations since 1989. "TruSecure continuously protects more than 700 customer sites in over 30 countries around the world." [1] After more research, K-Co's Security Manager found that TruSecure certified upwards of 95% of the various security products that fall within the categories of anti-virus, firewalls and intrusion detection systems. Some of the well-known security systems used on the market are Check Point Firewall, BorderManager Firewall, Panda Anti-Virus, Norton Anti-Virus, Tripwire IDS and Sourcefire IDS.

> ICSA Labs Firewall 4.0 Certification Criteria is the first program in the industry to test and certify products against the unique needs of distinct segments. Firewall product vendors can now submit products for testing and certification in the corporate, SMB or residential product categories. Each product is then tested against two sets of standards, the Baseline

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

Firewall Module and the Required Services Security Profile (RSSP) Module. – 2 (ICSA Labs Release)

More information is available regarding these products at www.icsalabs.com. The Security Manager of K-Co was impressed to learn that not only did TruSecure certify companies, but also had an armory of products certified to assist in attaining a certification. After further review of the company, Bill felt TruSecure was best qualified to help secure and certify K-Co. At this point, he scheduled a personal visit from TruSecure to determine the knowledge level of its promoters. During TruSecure's visit, Bill wanted to learn as much as he could about what steps TruSecure takes to complete the over all certification and what his employees' involvement would be during these steps. TruSecure is the only security certification firm that insures the systems that they certify. One more factor was added to the risk equation (Risk = Threat x Vulnerability x Cost), which TruSecure believes there is a cost associated with a particular vulnerability that has a related threat. Basically, after extensive testing from TruSecure and mitigation efforts on K-Co's part, each system that is certified would be covered by TruSecure in the event that security on these systems was breached. For each incident, TruSecure is liable to pay K-Co a monetary value to offset potential loss incurred by a security breech.

TruSecure also offers its own security knowledge and expertise to assist in trouble shooting how a system can be breeched, or could possibly be corrupted by one of the many threats that linger outside of K-Co's network. Another benefit to receiving the certification, a company will receive regular security alerts and updates delivered in the TruSecure Risk Monitor, which is a web-link set up during the certification process. TruSecure publishes an Information Security Magazine that assists its customers and subscribers by providing security tips and processes, plus some of the latest and greatest security devices on the market. In addition, TruSecure publishes an online security resource called NT Bugtraq for Microsoft-related security issues. Having these security resources at Bill's disposal and for the interest of K-Co, he felt TruSecure was definitely the security certification program of choice. From a cost analysis, Bill determined that TruSecure was the most expensive security certification program; a fact that almost prevented K-Co from using its services. After further analysis, the security benefit far outweighed the purchase price of this certification program. In addition TruSecure will commit to work with K-Co to maintain a high level of security to address the ever-changing security risks, associated with changes in K-Co's network and logical environments.

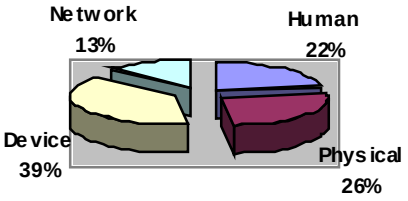
Companies can benefit in various ways by attaining security certifications. Certification programs not only assist in providing a level of security that can be considered hardened depending on how skeptical one is, but also can provide a level of liability for a company. Companies often pay exorbitant amounts of money to insurance firms depending on the type of service they provide and the level of risk the companies have. Security certification programs can help lower

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

this risk by mitigating the other components in the equation: vulnerability and threat. Companies can then prove to their insurance carrier that they are more secure by attaining the security certification, thus lowering their premiums. Companies can market the fact that they are certified through a proven security certification program to gain potential clientele. Most important, often companies can meet a level of security above and beyond where they were before they started the certification program.

Categories of TruSecure's Testing Process

The main categories that fall within TruSecure's Enterprise Risk Management Model are human, network, device and physical. An example of the model and a percentage breakdown of the main categories at K-Co required for certification are displayed as follows:



TruSecure's security testing covers an extensive range of security categories and characterizes risk into six concise categories. These categories are electronic, malicious code, physical, human, privacy and downtime, and are used in the risk formula for TruSecure's Security Essential program. A brief review of each one provides a basic understanding of the direction and how the risks conform to the testing conducted by TruSecure.

The electronic category encompasses threats to a system, whether internally or externally, to exploit a vulnerability such as sniffing, spoofing and poisoning. Malicious code is self-explanatory, and deals with viruses, worms, trojans, etc. The physical aspect of risk entails theft, surveillance and locks. The human category is possibly one of the most difficult ones to prevent and promote, as it pertains to social engineering, such as the inappropriate storage of passwords on sticky notes and policies. The fifth risk category is privacy, which encompasses access controls, levels and barriers systematically. The last risk category is downtime, which can be caused by many different threats such as DoS Attacks, Natural Disasters, systematic and human intervention. Below are the tests that were performed on K-Co in the order that they happened. These tests measured compliance with each risk category mentioned above.

During: Testing Begins (Perimeter Risk Assessment/Port Scan)

TruSecure initiated its testing process with a perimeter risk assessment scan to search for potential vulnerabilities on K-Co's network. Please note that prior to this scan it is always important to ensure some sort of change control process

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

has been completed and approved and then to notify the appropriate personnel what and why each test was occurring and when. The reason for such a step is to ensure that when the firewall administrator views the firewall logs and sees a barrage of TCP and UDP requests from a particular IP, he/she will be able to associate it with the TruSecure test. In the event that one of the TruSecure's tests brings down a system, he/she will know how it happened and who did it; a change control process will assist in these efforts.

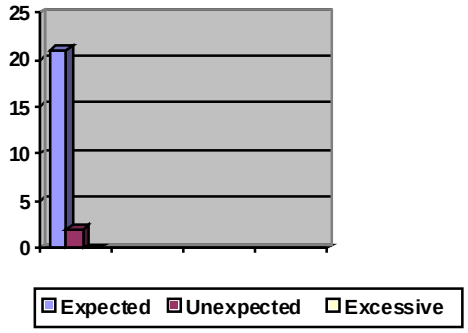
The perimeter risk assessment consists of two phases: the first phase is called a port discovery scan and the second phase is the vulnerability scan. TruSecure used ISS's Internet Scanner to scan for approximately 2200 TCP ports and 3850 UDP ports on K-Co's firewall. TruSecure used the IP range provided to them by K-Co's Security Manager for this scan. During this process they categorize the ports as expected, unexpected and excessive. Expected ports are those ports such as port 25 SMTP for mail services or port 80 for HTTP. Generally, these ports are open for business related activities and have business justification. However excessive ports are those that are above the limit of expected services that TruSecure has deemed acceptable; examples are IMAP, POP and DNS. Unexpected ports are above 1024, which may have been used for testing purposes on various products that are internal to K-Co, which should be closed when testing concludes.

With respect to unexpected ports there exists a threat to an internal network if it has not properly been segregated or subnet from the test network. In this case, a test box is not secured, as it would be in production, thus having various unnecessary services running on it, which can be exploited, through an unexpected port. TruSecure found a port like this that was actually opened to the K-Co production network for testing purposes. This is 'not a good idea.' Upon discovery, this port was closed.

The following graphical example displays the subject Discovery Scan. The numbers in the chart are used as examples for the purpose of this paper.

Expected: 21 services (discovered ports and services are:
SMTP – Port 25, DNS – Port 53, HTTP – Port 80, POP3 – Port 110, IMAP4 – Port 143, HTTPS – Port 443
Excessive: 0 services (No discovered ports and services where found)
Unexpected: 1 service (discovered ports and services are:
Terabase - Port 4000

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



During the next step, TruSecure ran a vulnerability scan on the open ports that were found during the discovery scan. TruSecure ran ISS's Internet Scanner and NAI's CyberCop again to find possible vulnerabilities. The vulnerabilities found are divided into four categories: intelligence, availability, integrity and confidentiality. The Security Manager at K-Co was impressed that this part of the testing not only discovered the vulnerability, but also matched it with the actual threat such as the Code Red Virus. The following are definitions of each category in addition to examples that were discovered during the vulnerability scan at K-Co:

Vulnerability Scan Categories

The first category, *intelligence* refers to the ability to learn about K-Co's assets or any company's assets through systematic processes, from information that is disclosed to the outside world. This would include technical data regarding system configurations and version information. An example would be discovering WWW Web Server version information, which can actually be tested by running a telnet session, trying to connect to port 80, then typing in a command such as 'GET /HTTP/1.0'. TruSecure offers possible recommendations to fix the vulnerability. A fix for the previous example might be to update the web server software to the newest version and apply the latest service packs. Another fix is to overwrite the syntax information so that proprietary information cannot be viewed.

Availability refers to hosts that are needed for legitimate users such as employees of K-Co or other clients. Famous examples of an availability attack are Denial of Service and SYN floods. Fortunately, K-Co had learned through security resources such as CERT or SANS how to mitigate this type of vulnerability, which prevented TruSecure from finding any exploits in this category.

Integrity defines weaknesses in a system, which can be exploited, thus overcoming any security barriers. Today viruses happen to pose one of the largest problems by exploiting system integrity. As mentioned before TruSecure

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

was able to associate particular vulnerabilities with known attacks. This was very beneficial since most security scanners generally provide raw output that can be quite cryptic to most users. An example that was discovered by TruSecure during their scan was the Code Red v3 backdoor vulnerability. Code Red exploited a known vulnerability in Microsoft's Internet Information Server, also known as IIS. The problem with IIS is that it can be a default install from another application and if not properly shut down or patched, can leave a network vulnerable. Possible recommendations for this vulnerability are to apply Microsoft patches, disconnect the Internet connection, if it is not being used, delete all copies of ROOT.EXE and delete Trojan files dropped by CODERED.C. Generally these items are not simply deleted from one place. Viruses have been known to scatter their exploits throughout many files of a system. Finally, if these fixes do not work, the Trojan has more than likely taken residence in the memory of the system. In this case, one would need to run a tool to clean the system memory. TruSecure suggested to K-Co's Security Department to learn more about the Code Red virus since this attack was quite intrinsic.

The last category is *confidentiality*, which involves client and employee data and other types of strategic information. This category can be found in almost all areas of IT. Whether authenticating to a system or transferring data, this information should be kept confidential and proprietary to a source. The volume of confidential information that K-Co handles pertaining to clients and their financial assets is monumental. Also, the sheer number of employees who administer this information can make it a challenge for K-Co's security group to ensure that confidentiality is in place. TruSecure was not able to discover any vulnerability within the systematic processes at K-Co pertaining to this category. In addition to locking down K-Co's systems, they were able to meet TruSecure's level of expectation by educating their employees. This was accomplished through such processes as new employee orientation and security annual awareness training. However secure this may make them, this does not mean that they are bulletproof; in fact it means the Security Department has a harder task in keeping themselves at this level.

Generally, from this point you can move onto the next test. Unfortunately K-Co's Security Department did not close out many of the previous vulnerabilities discovered in the perimeter risk assessment, so they had to work twice as hard to finish two scans at the same time. This exhausted the Security Departments resources, which in turn affected their daily duties. Unfortunately K-Co Security Department learned this first hand; thus made sure it would not be repeated. A suggestion would be to close out one test out before moving onto the next.

<u>WarDial Test</u>

In the next test that followed, TruSecure's outline was a WarDial on all of K-Co's publicly accessible analog phone lines to discover unsecured modems. Even with the strongest firewall in the world, all it takes is one improperly secured modem to bypass that firewall. This type of scan had never been run at K-Co

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

and its Security Department did not maintain a list of users who have modems on their desktops. TruSecure recommends that every company possess such a list. K-Co has a good Modem Usage Policy that states if a modem is needed it must be approved by the I.S. Security Department and used for business purposes only. When TruSecure conducted the WarDial, they based the WarDial on a range of phone numbers that K-Co's Security Department provided them. During the scan they conducted three separate checks, which verified the security of the modem and integrity of its authentication. The first check uses the phone numbers provided to scan for active modems on systems or desktops. The second check locates all modems connected to fax machines. The third check depends on the first two in which it looks for the user name and password on each modem and then decides whether they were carrier, fax or voice. The WarDialer conducts an assessment on the user name and password to determine their strength through brute force guessing. If the WarDialer finds weak passwords, they are noted in the report and considered a vulnerability to K-Co's network. The Security Manager was pleased to find that of the 35 phone lines, two modems were discovered, which had passwords that the WarDialer could not guess.

K-Co's Security Manager was concerned about this test, knowing that K-Co uses its phone lines and modems for critical business needs and could not afford down time during these tests. In preparation, Bill did research prior to the WarDial to find out the likely duration that it would take to test each line. TruSecure explained that during the WarDial they will call the number and if it connects, the Dialer will distinguish what type of connection and then test the integrity of the authentication in less than a minute. It is unlikely that a "brute force crack" can be performed in this short time frame. If the phone line is busy, the Dialer will try several times before moving on to the next line. 'A very interesting test'! The Security Manager was sure he would personally be conducting a test of this nature in the near future.

<u>Unexpected Attack During the Certification Process</u>

Prior to conducting the next test, K-Co discovered that a sister company of theirs had been attacked through DNS Poisoning. A client who had difficulties connecting to this company's web site discovered the attack. K-Co's sister company, which already had been certified by TruSecure, held a conference call with TruSecure and K-Co to discuss recommendations to mitigate and prevent this type of attack. DNS poisoning is a malicious attack intended to change the IP address associated with a web site address (URL). DNS poisoning can be achieved in a number of ways. These methods were discussed in joint meetings between K-Co's Security Department, TruSecure and the company that fell prey to the attack, examples are:

- By exploiting a buffer overflow in the DNS implementation and altering the DNS database entries.

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

- By spoofing the response to a query from a legitimate DNS server by guessing its response identifier.
- By exploiting a vulnerability in versions of some older DNS implementations that allow a DNS server to upload DNS records relating to a domain for which it is not authoritative
- By spoofing an authoritative DNS server.

It was also discussed that DNS poisoning can be performed manually. A Security Administrator of K-Co researched and discussed with K-Co's Security Manager how this was accomplished. Basically, an exploiter will send a bogus request to the domain name registrar using a spoofed email address requesting a change of IP address associated with a domain name. If the domain name registrar does not have appropriate security practices in place backed by a policy, the spoofed email address would be considered enough verification to initiate the change process. Normally, a domain registrar would then send back an email with a tracking number to the registered domain name administrator verifying that changes were going to be made to the DNS entry. This would normally alert the administrator to any foul play, and also provide him/her a method to stop the process using the tracking number. Another simple tactic would involve resetting the password used to make changes to the DNS entry. With an insecure domain name registrar, one would send a contact form with a new password, along with a fax that authorizes the registrar to process that form. By scanning a company's letterhead this can become more credible.

> DNS servers will "recursively" resolve DNS names. Thus, the DNS server that satisfies a client request will become itself a client to the next server in the recursive chain. The sequence numbers it uses are predictable. Thus, an intruder can send a request to the DNS server and a response to the server forged to be from the next server in the chain. It will then believe the forged response, and use that to satisfy other clients. – 3 (FAQ: Network Intrusion Detection Systems)

The following are some recommendations discussed by K-Co's Security Department and TruSecure's security engineers to assist in the prevention of DNS poisoning at K-Co's location and mitigation efforts for their sister company. Verify that the domain registrar has the proper verification policies and procedures in place to ascertain whether change requests are truly being received from the registered administrator. Alternate methods to communicate this information are SSL-encrypted web pages; also requiring a PGP signed and encrypted email to make changes to domain information.

Consulting the domain name registrars' server administrators to ensure that their servers have been secured against DNS spoofing, perhaps through the use of DNSSEC or other means. Also verify that the registrars' DNS implementation (normally BIND) is up to date, and made secure. K-Co can also perform a whois lookup on its domain names frequently and consistently to verify that the DNS

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

entries have not been tampered with. Finally adding a string of text to the Meta Tags of web pages (P!32983HKg3948# for example). Meta Tags are most often used by Internet search engines to look for keywords to create a list of results from a search. K-Co can perform an Internet search regularly from various search engines using that text string. Then by following up on the results returned K-Co might find another web site that contains the string. This would provide the conclusion that someone has duplicated K-Co's web content and is redirecting users to that site. The following recommendations are currently being researched for possible implementation. Following these steps K-Co continued on with the remaining tests.

Back to Testing - DRA (Desktop Risk Assessment Test)

The next test was performed by K-Co's own Security Department, but was facilitated by TruSecure. K-Co's Security Manager was unhappy about doing this; Bill felt TruSecure should be conducting every step of every test as part of its contracted fee. This test was called Desktop Risk Assessment Test; it is a homegrown application developed by ICSA Labs. It needed to be loaded onto the K-Co network so that it could view each user's registry profile as he/she logged on. Once the data was collected, K-Co compiled the information into an XML file and sent it to TruSecure. The file was then placed into a more detailed format for K-Co's Security Department to work with. The K-Co Security Department learned that as a result of this application, when a user signs on, a black box will appear on his/her monitor for a split second, and then disappear. This split second was enough time to cause panic at for the users at K-Co. The Security Manager knew that the Help Desk would be inundated with calls from frustrated users, thinking something was wrong with their computers.

When the application runs, it looks at the desktop's registry profile on each user and determines whether security processes in the registry are compliant with TruSecure's recommendations. An item that the scan picks up is whether or not the screen saver is activated. It also verifies whether or not the screen saver is password protected. K-Co has a policy that states that every user must have a password-protected screen saver and it must time out according to the time stated in the policy. TruSecure's recommendation was the screen should be activated in 5 minutes. This can be difficult tell the rest of the company even though the Security Manager would like it to be much less. The Security Department had already established a time out of 10 minutes, which was stated in their policy based on business needs. This would accommodate phone representatives who deal with clients and would not like to sign on every time a question is asked over the phone.

There's a quote that has been said many times that 'security is not convenient, but compromises can be made.' When a compromise is made, security should never be an afterthought. By keeping security in the forefront of any security breech, further compromise can be mitigated. During the screen-saver scan, K-Co met all of TruSecure's requirements except one, which was the time out

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

period. TruSecure does not base its decisions on one company alone. They base their decisions on statistical facts generated through large samples that provide security risk, and the vulnerabilities and threats associated with them. K-Co needed TruSecure to make an exception to the rule since K-Co required a longer timeout for business needs. K-Co's Security Manager was required to provide justification for this part of the assessment. TruSecure evaluates the justification depending on the level of risk and makes a decision whether to pass K-Co or not. TruSecure generally makes the evaluation and decision of an attestation made by representatives from any company before final certification is granted. If the representative at TruSecure feels it needs further review the attestation is sent to a decision board for review and final decision.

The next part of the scan checks the security-level settings for the Internet browser on each computer. TruSecure recommends a level of 'Medium' for an Internet connection. They believe that this will provide adequate security and still allow flexibility to browse the Internet. It is a standard that that K-Co has a security setting of medium and is reinforced by its security policy. Once this setting is established no one but an administrator with privileged access can change this setting. K-Co passed this part of the assessment with flying colors.

Following this scan, the tool will look for anti-virus protection at each desktop. This can be considered the most critical scan of them all. Not saying that the other scans are less important, but because of the exorbitant number of viruses that are currently floating around on the Internet this scan is important. The application scanned for whether the desktop has virus protection and if it had been updated with the most current DAT file. The Security Manager at K-Co makes it a point to layer his anti-virus systems. K-Co currently employs a three-tier anti-virus protection strategy and policy. The first layer, which is the outermost layer, is the gateway layer. This is the first line of protection, scanning incoming email prior to it reaching the email server. The next layer is the server layer, ensures that every server deployed has anti-virus protection on it. The last layer and the most difficult to administer is the desktop layer.

The TruSecure desktop scanning tool assists the Security Department in policing their anti-virus software. It looks at the desktop to decipher whether anti-virus software is installed and verifies if the DAT files are current. The scan that was performed did not find any system lacking anti-virus software at K-Co. The Security Manager was surprised to find out that some of the systems had DAT files, which had not been updated in either 30, 60 or 90 days. Bill and his group acted on this problem immediately. By the end of the day every system had current DAT files and going forward all desktops were systematically updated on a daily basis.

The last scan located the total number of desktops that had modems connected to them. TruSecure's standard states that no more than 10% of all desktops shall have modems on them. The reason for this is to reduce potential

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

vulnerabilities such as weak passwords on modems or modems set to auto-dial. If a company exceeds 10%, it will have to provide justification for the additional modems according to their business use. K-Co did not need to provide justification; fortunately they fell below the required 10% and passed this stage of the test.

1st On-Site Assessment Test

TruSecure conducts two on-site security assessment tests during the process of the certification. The following discussion identifies the steps that were taken during the first on-site assessment test to validate TruSecure's essential practices. When TruSecure came on site they brought a third party tool that was used to assess security measures on K-Co's network. The tool, CyberCop, is a network-scanning tool that looks for vulnerabilities associated with intelligence, availability, integrity and confidentiality. The vulnerabilities that were discovered by this tool are generally associated with out-dated systems, versions and insufficient security patches. K-Co's Security Department kept busy for several weeks due to this assessment test, which found more vulnerabilities than were previously known by the K-Co Security Department.

For the purpose of this paper, examples will be provided to better understand why certain vulnerabilities appeared and the steps that were recommended to mitigate them. Within the report produced by CyberCop was an *intelligence vulnerability* associated with an FTP Banner Check. Many implementations of FTP servers provide information about the server to FTP clients who attempt to log on to the system. Basically the banner on this service provided intelligence such as version information, which a hacker could use to exploit this system. The banner read *'220 javaserv3 Microsoft FTP service (Version 4.0)'*. These vulnerabilities can often be overlooked since the banner can be set up by default. If no one bothers to change it during the setup it will get pushed out unsecured. While the banner should be used to present warnings to attackers, it more frequently provides information to an attacker about configurations of the system.

The first of TruSecure's recommendations is to find out whether or not this service is needed on this particular system. If not shut it down. If the service is required TruSecure recommends changing the banner to read 'Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.' Putting this in big bold letters doesn't hurt. This will assist in deterring hackers from accessing a system and it will also act as a legal barrier if the system does get compromised, by stating that K-Co specified only authorized access is permitted. Action was taken immediately to change or remove all banners that contained information that could be used to gain access to K-Co's systems. The Security Manger took this one step further and required this change on all logistics documents at K-Co. This way, if TruSecure recommendations have not

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

been met, Bill will not sign off on the logistics document to approve the installation of a project. This recommendation should be considered at other companies.

An example of an *availability vulnerability*, discovered during the assessment, was the 'WinGate POP3 Proxy Username Overflow Check.' Basically, certain versions of the WinGate POP3 proxy contain a buffer-overflow vulnerability. If an attacker gained remote connectivity to this server, he or she could render it useless and crash the server. Since WinGate does not check the length of the arguments submitted to the USER command, a hacker could simply submit an unusually long user command to overflow the internal buffer. As a recommendation, generally POP3 is not necessary on K-Co's systems, so they disabled it immediately. If it is required, update the systems with the latest version of WinGate, which generally contains the fix.

There were quite a few examples of *integrity vulnerabilities* that were discovered during the assessment test. This was an area that needed much attention, but yet can be easily overlooked. Most of the integrity vulnerabilities are associated with excess services running on a machine, that either needed to be turned off because they weren't being used, or patched. Unfortunately when companies sell a product, they want to market all of the benefits it can provide for a client. By having these services readily available and running by default, clients feel as though they are getting a great product and more for their money. The security Manager at K-Co would most likely agree with other security professionals that extra services or default services could be more of a risk than a benefit.

An example of an integrity vulnerability discovered by CyberCop during the assessment test, is the 'Mail Relaying Allowed' vulnerability. Allowing mail to be relayed through their hosts can possess quite a problem. Mail relaying can increase the load on the mail server, which can provide quite the attraction to spammers who usually send hundreds of thousands of email to their audience, thus utilizing the victims mail server to relay the messages. To compound the problem, the recipients of mail from this server will receive that spam as well and will think that it has initiated from K-Co's mail server. "Using an open mail relay from another site is attractive to the intruder because accountability is far less enforceable." [4] There are various Internet sites that provide direction on how to secure an email server. A site that is highly recommended is www.mail-abuse.org. This site provides steps on how to secure a mail server from third-party relay and lists examples of spam that can be received. If K-Co decides not to use this service and secures it according to the web sites recommendations, they need to reconfigure the SMTP software on the host to disallow mail relay. If the mail service is not needed, disable SMTP on that host.

Another example of an integrity vulnerability is the 'rpc.statd link/unlink check' vulnerability. The statd monitors the NFS (network file system) file-locking status. NFS provides remote access to shared files across the network. The

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

NFS protocol is transparent and is portable across different operating systems, network architectures and transport protocols.

> The called rpc service may be a local service on the same machine or it may be a network service on another machine. Although the form of the call is constrained by rpc.statd, if the call is acceptable to another rpc service, the other rpc service will act on the call as if it were an authentic call from the rpc.statd process. – 5 (CERT/CC)

There are some versions of statd that can be forced to unlink or create files as root remotely. Knowing that NFS is a program essential to business practices, TruSecure understands that K-Co just cannot shut this service off. Therefore TruSecure requested a business justification for running NFS, which is reviewed by their Security Board. Since this service was used for trouble shooting and business related activities, justification was required. K-Co's Security Manger drafted an attestation for this vulnerability, which was approved by TruSecure. More information on this type of vulnerability, as well as fixes can be found at www.securityfocus.com.

The final example of an integrity vulnerability was discovered during on-site assessment at K-Co. This is the 'FTP file write permission check'. During the scan, TruSecure checked the anonymous FTP directory hierarchy for writable files and directories. Directories and files that are writable on K-Co's FTP server can expose their network to being used as a pirated software storage site. The following are examples of files that were found to be writable on the ftp server:

/SWSdb/UDSC/1.2.08:
'-rw-rw-rw- 2 root root 1862997 Jun 30 1999 udsc.z'
/SWSdb/UDSC/1.2.08:
'rw-rw-rw- 2 root root 66532 Jun 29 1999 setup.ins'

TruSecure strongly recommended disabling anonymous access to the FTP server. If K-Co felt they needed anonymous access for business purposes, they needed to implement restrictive permissions on all files and directories accessible by anonymous user. Also if there is a need to post to the FTP server, only one directory should have write access for this purpose. Users should not have the ability to create new directories. Finally, only the administrator-level accounts should have owner permissions to retrieve files. Also by making FTP root directory and its subdirectories owned by root, part of the system group, and protected so that only root has write permissions, secures anonymous FTP services. Other recommendations are setting access controls to the posting directory, limiting the amount of data that can be transferred in on session, and increasing auditing functionality to provide sufficient monitoring. K-Co did not require anonymous access for their FTP connections so it was disabled during the on-site assessment test. K-Co also ensured any FTP connection required login information such as a user ID and password.

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

The last vulnerability type is *confidentiality*. The example is the 'FTP – bounce attack', which was a known vulnerability at K-Co. This particular FTP service was found vulnerable and would redirect data while masking the attacker's origin. Instead of opening a connection back to the source IP address of the FTP request, the port and destination IP can be altered in order to circumvent export restrictions and access control. If this service was not needed, TruSecure recommended deleting it. If needed, K-Co needed to install all relevant upgrades and patches. After further research K-Co found that they did need this FTP connection. The Security Manager ensured that the latest patch was acquired and installed, while TruSecure was on-site during the first assessment test. Unfortunately many more vulnerabilities were discovered during the first on-site security assessment test. K-Co definitely had their work cut out for them. The on-site assessment test allowed K-Co to proactively secure their systems and the services that run on them according to the vulnerabilities that were found. This is definitely a better approach than waiting to be hacked and dealing with the consequences later.

2nd On-Site Assessment Test

TruSecure planned a second on-site assessment test, which reviewed the human factor of their essential practices and physical security at K-Co. The Security Manager at K-Co felt TruSecure had been quite impersonal prior to this test. Until this point Bill had only dealt with the paperwork that had been created by TruSecure's security scanners. So needless to say he looked forward to this test, now he could actually hear what a human being had to say about the security at K-Co. In addition to evaluating the human factor, which focused on company security policies and practices, a physical walk-through of K-Co's facility was required.

TruSecure brought on-site a list of items pertaining to physical security, which K-Co was either required to have or provide an alternate means that would need approval. An item that TruSecure required was the use of electronic badge identification card readers. This was a necessity for K-Co as they worked in a busy rural part of town. In addition to having the badge readers, it was mandatory to create and monitor access levels to critical parts of the company, such as the Data Center. Logs needed to be maintained and stored offsite, in the event that a disaster occurred such as a fire. Also in the event of an incident, it would be necessary to pull logs of who went where and when. K-Co's Security Manager had drafted a Physical Access Policy prior to TruSecure's visit, which outlined many if not all of the factors that TruSecure required for badge reader access. This policy outlined what steps were required for maintaining a physical identification system at K-Co. The administrator from TruSecure approved this policy, which allowed K-Co to pass this stage of the test. Another item required by TruSecure was the use of a surveillance system in the Data Center. Fortunately, K-Co was proactive in this step and had a surveillance system in place prior to this visit. TruSecure did provide an exception to this rule, which was to have a physical log of visitors. In addition to having such record, each

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

visitor was required to have an escort. TruSecure does not generally recommend this as an alternative, but the administrator from TruSecure stated it could be used in addition to surveillance cameras. Paper logs of who entered the Data Center; do not provide the security team with the ability to identify someone who committed theft first hand. Such logs only provide the time the person signed in and signed out. On the other hand a surveillance system can identify the perpetrator first hand and provide solid evidence during an incident. Another items TruSecure tested were whether or not server racks in the Data Center were locked. This reduces the possibility of someone accidentally or purposefully harming a system from the consol, or physically tampering with the device.

TruSecure focused in great detail on the need for K-Co to have a thorough and up-to-date policy manual. The following list of the policies were required for the TruSecure certification:

–Firewall Policy
–Anti-Virus Policy
–Authentication Policy
–Data Disposal Policy
–Continuity Policy
–Incident Reporting Policy
–Privacy Policy
–Wireless Policy
–Physical Access Policy
–And Remote Access Policy

These are issue-specific policies, but allow for a range of items to comply with each one of them. TruSecure recommends that these policies should be established for all companies to ensure compliance with state and federal regulations.

One final item that TruSecure verified and tested was if K-Co monitored and logged critical systems and applications. Auditing security logs and system logs as a practice can be considered the backbone to understanding what is happening on a company's network. K-Co currently employs a security checklist that outlines all system logs and security logs. The checklist is set up to define when, who and how these logs are to be monitored. K-Co also possesses a centralized security-logging server, which captures various logs throughout the network. These logs contain failed attempts to access a system, lockouts, root access attempts, su-root access attempts, unscheduled reboots, system shutdowns, as well as access attempts on specified systems. This way, K-Co can trace a possible intruder much easier with the logs maintained in one repository. TruSecure reviewed these processes and passed them for certification.

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

Closing of Testing Process

After K-Co was in compliance with TruSecure's Essential Practices for their internal network, a follow-up Perimeter Risk Assessment and modem WarDial was required, if they hadn't been conducted 30 days prior to the conclusion of the certification process. K-Co did have to schedule a follow-up perimeter scan. Fortunately K-Co conducted a thorough job fixing the previous vulnerabilities, and ensured that all systems added to the network would not duplicate previous vulnerabilities, or add new ones. TruSecure confirmed that no new vulnerabilities were discovered and passed K-Co to close out all testing processes. K-Co properly mitigated all of the vulnerabilities from the on-site assessment, and received approval on their attestations by TruSecure's security board. K-Co complied with 76 of TruSecure's Essential Practices that apply to their electronic and physical infrastructure. By addressing all the Essential Practices, K-Co was granted TruSecure's Enterprise Certification.

After: Follow-up Recommendations for After Certification

TruSecure provides many recommendations on how to mitigate and fix a known problem, although, they did not offer many suggestions for K-Co to test their own systems, since they would rather a company use their services. K-Co's Security Manager realized that his Security Department needed to be running its own security assessment tests even if he didn't have enough staff. Bill began to research the types of tools that could assist in this process. Some popular examples are ISS Security scanner, RETINA's network security scanner and SATAN. Many of these products are free while some K-Co may have to purchase. This way K-Co can set up periodic security checks of their network to find vulnerabilities, and patch them before TruSecure runs their next security assessment test. This will ease the pressure of maintaining the certification. K-Co should also subscribe to as many vulnerability news groups to stay abreast of new patches, fixes and versions. This also enhances the education of K-Co's Security Department on vulnerabilities and the threats that prey on their network.

In Conclusion

A company can benefit in many ways by recognizing the importance of security certification at the corporate level. TruSecure's security certification program assists in ensuring that the integrity of one system can be matched by the integrity of the organization as a whole. Since the conclusion of the certification process TruSecure has provided K-Co with a management summary outlining the complete certification process. This report can supplement security information required during other audits, such as the FDIC, State and Banking Commission and other private audits. K-Co was also provided a seal of approval that it had completed the certification process. This seal can be used on marketing material for future clientele. As mentioned prior to the certification process, K-Co can also reduce its insurance premiums, proving that it has enhanced its security program to a notable degree.

When a client looks for a financial firm to manage their individual retirements accounts, a company such as K-Co who has a proven security program,

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

supported by TruSecure Corporation would be their likely choice. The client will know that a certain degree of protection has been established to protect their assets. The degree of protection in this case has been tested and measured by such disciplines as audit and penetration of technology, physical and administrative processes at K-Co. In addition, a certification programs assist K-Co in maintaining levels above and beyond competitors for their security programs, through such measures as protection, detection and recovery.

Resources

1 Corporate Info. "TruSecure Corporate Information." URL: http://www.trusecure.com/corporate/ (16 Dec. 2002).

2 ICSA Labs Release. "ICSA Labs' Firewall 4.0 Certification Criteria is the First-Ever Customized Program to Test Products Against the Unique Security Needs of Three Distinct User Groups." 3 Dec. 2002. URL: http://www.trusecure.com/corporate/press/2002/firewallcert120302.shtml (16 Dec. 2002)

3 Finley, Ian. King, Brian. Hernan, Shawn. "Open mail relays used to deliver 'Hybris Worm'." CERT Incident Note In-2001-02. 2 March 2001. URL: http://www.cert.org/incident_notes/IN-2001-02.html (18 Dec. 2002)

4 CERT/CC. "Vulnerability in statd exposes vulnerability in automountd" CERT Advisory CA-99-05. 9 Nov. 1999. URL: http://www.cert.org/advisories/CA-99-05-statd-automountd.html (18 Dec. 2002)

5 Graham, Robert. FAQ: "Network Intrusion Detection Systems." Version 0.8.3. 21 March 2000. URL: http://www.robertgraham.com/pubs/network-intrusion-detection.html#DNSsequencespoof (18 Dec. 2002)

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

Last Updated: May 19th, 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**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**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**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**