# Global Information Assurance Certification Paper

**Case Study in Information Security:**

# "Powerless Over Poor Security – The Missing Foundation"

**GIAC SECURITY ESSENTIALS CERTIFICATION**
**PRACTICAL ASSIGNMENT v1.4b**

**DANIEL_MELLEN_GSEC.DOC**

**SUBMITTED SEPTEMBER 2, 2002**

## Table Of Contents

## Introduction

*Enter stage, right, Company X (CX).* Security was not a major consideration for CX; they installed a firewall in the late nineties, like most companies and didn't give much more thought to it. After all, their primary focus was research and development, known for producing reference and research data for many commercial scientific and governmental groups. Why would anyone want to break into their systems?

*Enter stage, left, Angry Hacker Andy.* Andy sat at his computer desk amidst a pile of empty Doritos bags, Mountain Dew cans, matches and a few employment rejection letters. "Why didn't anyone want to hire me? I have done cutting edge building fire and explosives research for school." He asked himself. "They think they are too good for me? …I'll show them." He picks up his rejection letter from CX and reads aloud. "Dear Andrew, I regret to inform you…" strikes a match and lights the bottom of the resume-grade paper and drops it into the aluminum trashcan by his CPU and says aloud, "Dear Company X, I regret to inform **you**…"

And that is how this story begins…

## Abstract

When Company X started, they struggled to get enough funding and venture capitalists' money to purchase all of their laboratory and computing equipment; there was no room for luxuries. The bare minimum was done to remain operational and profitable. A few years later, some scientists noticed that some of the systems they maintained had been tampered with. Some data was missing and other data had been manipulated. They had been compromised. The CEO was furious and when they caught wind, so were the investors. This was to never happen again. *Enter stage, center, Dan the Security Consultant*.

Upon review of the organizational chart, the administrative manual and some network scan results, it was clear that there was an ugly, fundamental problem at CX. They had failed to plan for security. The products of this failure were vast and would require a sizeable paradigm shift within the company in order to be remedied. There was no guidance, policies or procedures for acceptable use, patch, upgrade or any other area covered by basic policies. They had a lone Chief Security Officer (CSO) who was responsible for little more than the firewall administration and reported to a manager in IT computing. The absence of policy and weak misplacement of the security authority further resulted in out of date applications, modems connected to machines behind the firewall and the rampant deployment of insecure services.

There are several approaches to this problem, two of which I chose to employ. The first was coming up with a "quick hits" list of high risk, high impact, likely threat issues that could be dealt with in a short timeframe. The second was developing a set of policies, procedures and organization restructuring options, retrofitted to the current operation of the company. The goal was that they would minimize the impact on the day-to-day operations and would be as transparent to the scientists as possible, yet would raise the level of security to a reasonable and acceptable level. Additionally, a training and awareness program was implemented to compliment and justify the policies to those affected. By fixing the root-level problems, proper operating behaviors would cascade out and eventually overcome the less security conscious activities currently in place.

The security posture of Company X improved dramatically with the implementation of the abovementioned solutions. The number of compromises, the location of their occurrence and their impact was contained and managed and pleased both the CEO and the investors. The level of understanding amongst the employees increased as well as the consistency of processes within the company and its various divisions.

This all sounds like a very easy process, condensed into a few paragraph-long abstract. The following sections will go into much more detail about the state of affairs, the identification of and approach to the problem as well as the issues inherent in those processes. It will also discuss the implementation and results, the successes and troublesome areas throughout the solution completion. There is also an extra section at the end of this case study that details some "lessons learned" from this and other security engagements.

## Before

As a result of security being absent in the planning stages of the company, proper policies and procedures were not developed, the security organization was not properly empowered and the overall security posture was not at an acceptable level to defend against a possible attack. Several subsequent products of the lack of security considerations were vulnerable applications, insecure modems and unnecessary services.

### *The Organization*

The role and placement of the security authority, in CX's case, the CSO, was weak and inappropriate. The placement of the CSO in the organizational chart had him reporting to a manager in IT computing. This manager reported to a director, who reported to a Vice President, who, finally, reported to the CEO. There was no one under the CSO and he had no authority to dictate any security measures to the people at CX. This arrangement would never be effective.

Hypothetically, if the other identified problems been considered, had policies and procedures been created, the CSO still had no power to enforce them. His position granted him no leverage and no support to implement change or ensure compliance. The policies and procedures would be ineffective and essentially moot.

The limited responsibility offered to the CSO was also very inhibiting. The CSO was pigeonholed into firewall management and did not evaluate the security posture of CX outside of this scope. Multiple facets of host, network and physical security were completely ignored leaving numerous vulnerabilities and points of failure open to exploitation.

### *The Guidelines*

It is said that policies and procedures form the backbone of any good security program [1]. CX did not have any written security procedures or policies and, therefore, provided no guidance to its personnel regarding acceptable means for conducting business in a secure and orderly manner. Users were able to download and install a multitude of programs from anywhere on the Internet on their work computers. They were not admonished against installing modems and dial-up access software to allow them to work from home or use CX as an Internet Service Provider. Additionally, they were not required to upgrade versions and patches to operating systems or application software on their workstations or servers.

Several instances of trojaned software applications, unpatched operating systems and non-business applicable software were found on CX workstations and servers. When war dialing, modems were discovered that did not provide any authentication or identification and blank and null PC access software passwords were uncovered. These machines sat behind the CX firewall and represented enormous risks to the company's scientific data.

Once these follies were discovered, there was no simple way to resolve them; there was no policy to point to that said that they were not allowed. No procedures defining acceptable use or

modem restrictions preventing unauthorized and unauthenticated access to the CX internal network. People had routines and were accustomed to doing things a certain way.

There was no training and awareness program because there was not material to train people on and of which make them aware. There was no real source of written or human security guidance and, therefore, no one to direct the development and implementation of a training program. CX employees were not aware of the risk at which they were putting their company.

### *The Products*

Resulting from the lack of policies and procedures and a powerless CSO, CX suffered a gross abundance of poorly programmed, trojaned, out-of-date and unnecessary applications and services that further degraded their pitiful level of security. Following some system and network scanning, I discovered that they had insecure services running and out of date applications both of which provided avenues of entry into their protected network.

Scientists in the building fire and research division noticed that some of the data they produced had been tampered with and other data had been deleted altogether. This issue was raised in a meeting and eventually came to the attention of the CEO. There was little auditing enabled on the systems and the knowledge of what to do after an incident was non-existent. For these reasons, there was not enough forensic evidence to prove that Angry Andy was the culprit – but it is alleged and widely accepted.

The breach was born out of the lack of application patches on SSH which afforded the attacker enough access to steal and delete valuable scientific research data. The firewall worked as expected and likewise did the security measures of SSH. The problem was that, because patches had not been applied, the version of SSH that was running was vulnerable to attack and compromise.

### *The Assistance*

The GIAC Security Essentials course outlined the proper practices that lead to secure environments, such as defense-in-depth, principle of least privilege and other guiding axioms. These ideal situations, when compared to the current state of affairs at Company X, led to a series of deltas. These discrepancies represented a set of risks that required attention and action.

Additionally, the GSEC course helped instill the ideas that upper management approval and support is required to be successful at implementing changes of this magnitude. Moreover, the course educated that policies and procedures are the foundation for any good and effective security program. Without these, the difficulty of pushing down requirements, implementing security best practices and enforcing the policies becomes a monumental, if not impossible, task.

## During

### *The Approach*

The approach that was chosen was intended to be a long-term solution to the problem, attacking the source of the problem. However, the problem with the long-term solution was that there were several short-term fixes that were identified that would not require the same extended duration. Given this fact, I came up with a "quick hits" list of high risk, high impact, likely threat issues that could be dealt with in a short timeframe. This represented low-effort "wins" for CX that could be realized immediately. Not only did this improve the overall security posture of Company X, it gave them instant gratification that showed that progress was being made, while the long-term wheels of change were set in motion. The long-term effort required cultural and habitual changes in the way that CX employees conducted business and the rules that they followed and would take time to fully adopt. The balance of these two approaches provided success and vision to securing CX.

The first step in the process of fixing the problems with CX was to analyze the problem. Tracing the problem as far back as possible helped identify the root cause of it. The following chronological flow is the result of a meeting with CX executives. It outlines the problem from root cause to final result:

> No planning for security in the initial phases of the company design • Poorly placed security authority • No guidance to aid people with a path to follow • No policy to enforce when path was not followed • Bad practices that were difficult to reverse • Security shortcomings cause poor security posture for CX • Vulnerable systems that were easily compromised • Data integrity issues for scientific data • Management and investor fury • Negative publicity and reputation tarnishing • Culminates in investor distrust and company volatility.

This flow defines a clear path to the root cause and enumerates all of the effects that resulted from the original decision (or lack thereof). This process also involved various members of upper management and illustrated to them the problems that resulted from their lack of foresight regarding security.

### *The Short Term*

Based on the abovementioned problem analysis, several steps were identified as being short-term solutions that would immediately have a positive impact on the security of Company X. The CEO approved and delivered a list of acceptable versions of applications, operating systems and services deemed required for business operations, per the CSO's recommendation. This message was delivered to all of the Vice Presidents, Division Directors and System Administrators. A two-week deadline was instituted for the submission of exceptions to this rule. Each Vice President was accountable to the CEO and had his or her Division Director assume responsibility for signing and obtaining the signature of all direct report System Administrators to ensure compliance. Presumably, this would eliminate a large number of the vulnerabilities currently

exploitable to gain unauthorized access to CX.

In addition to this step, and more importantly, the position, role and responsibility of the Chief Security Officer was redefined. In order to effectively run a security program at CX, the CSO was moved from his current position to one affording much more authority. The position was removed from IT computing to the security office and reported directly to the VP of IT. This move placed the CSO as a peer to all other Division Directors in the company. This was done to reduce the amount of power struggles and conflicts that would occur if a less authoritative position were trying to dictate requirements to others. To assist and support the CSO in his new position, two special skilled security analysts were hired for distinct reasons. The first was a corporate security policy expert and the second was a proven training and awareness program instructor. These two individuals worked closely with the CSO to implement a security plan and enlighten the employees of CX to the changes and the reasons behind them. These two steps were necessary to ensure the success of the security program going forward.

The repositioning of the CSO also required a redefinition of the role. The CSO's scope of responsibility was expanded from just the firewall, to include applications, services and operating systems in CX's publicly accessible network, as well as, the compliance enforcement of the policies discussed later. The two individuals hired into the security office followed the direction of the CSO.

Extensive public-facing system scans were performed because they were recognized as the first line of defense/entry into CX. These are the most visible and vulnerable systems to outside hacker attacks – a problem that burned the company in the past. These vulnerability scans were followed by a company wide risk assessment. This exercise not only helped the participants get in the security frame of mind, it also helped to determine individual plans of action, both short and long term.

The location and means of storage for scientific data was assessed in the short-term. Given the recent break in, it appeared as though this was a tempting and vulnerable target. This data was seen as the company's crown jewels behind the scientists themselves. Data storage on publicly accessible machines was discouraged and the use of integrity checking and read only media was promoted. The benefits of Tripwire for servers [2] was explained, such as file and system integrity, and its applicability to CX and its research data was discussed. The validity of data could be maintained as long as it was properly stored and monitored. Additionally, read-only media was investigated as an alternative to traditional read-write media. The use of writeable CD-ROMs for data publishing for customer access was planned.

Systems that were inside of the boundaries of the publicly accessible network were required to pass the system and network vulnerability scans discussed above. These scheduled scans were run once each quarter and Vice Presidents were accountable for any failures, per their previously signed assurance form. These systems were hardened in accordance with the guidelines set out by the National Institute of Standards and Technology (NIST), the National Security Agency (NSA) and the Center for Internet Security (CIS) [3].

The combination of all of these steps defined the short-term solution for securing CX and provided early motivation for the long-term security implementation.

### *The Long Term*

In looking to root cause of problem, several issues were raised that required a major change in the behavior and normal operations of CX. Without a fix at that level, the changes and improvements that were implemented would only be temporary and the long-standing problems would continue to resurface. In essence, by implementing a serious, long-term plan that attacks the root of the problem, the solution was much more permanent and effective, versus acting as band-aids on a larger problem.

One of the main efforts of the long-term solution was born out of a decision started in the short-term time frame. The creation of a training and awareness program and someone to run that program was crucial to the program's success. The adoption of a security program where previously there was none required a certain amount of explanation of what was being done and why it was being done. This was the primary function of this component. The informational services that originated here helped to ease the implementation and growing pains of a paradigm shift within CX. Push back was anticipated when changes were introduced to the existing habits of the company, however, justification for the changes and the benefits of the changes were recognized and there was much less friction in reaching compliance.

The implemented training and awareness program led to the recognition and adoption of security industry best practices. It was the responsibility of the CSO to research, recommend and enforce these practices. Additionally, policies were aligned with the recommendations of the CSO. Policies, including acceptable use, system scanning, modem restrictions, patch and upgrade management for applications and operating systems and public network security were all implemented. Signatures from all Division Directors and System Administrators were required as to their recognition and understanding of these policies. Reversing years of habit does not happen overnight or without thoroughly explained justification and that is precisely what this program and solution intended to address. Policy and procedures were the focus of many of the early training and awareness sessions. The realization that some things could happen immediately, while others would take time and explanation was instrumental in the successful implementation of CX's security program.

This solution was chosen because it combined the best parts of the short and long-term solutions. Either solution could have been implemented on it's own, however, would not likely have been as effective because of the different targets to which each were tailored. The combined program necessitated upper level management agreement and support to be successful due to the magnitude of the changes. After the problem-tracing session explained at the beginning of this section and supplying examples of other corporations that chose one path or another CX executives chose the correct path.

By increasing awareness, security began to be considered in many aspects of CX's employee's business lives. This was proof of a positive outcome and an increased sense of security. For example, in the design phase of scientific applications and processes, security began to be a topic

of discussion. This was a monumental feat. Typically, security would be brought to the table after the development was completed if there was a requirement for security that was overlooked and would have to be retrofitted into the application. This shift represented a large step for the security organization in reaching its goal of security integrated into all aspects of its operation. Many of the previous follies acted as "lessons learned" exercises, not to be repeated in the future.

The steps, outlined above, that were employed to solve the problem were blatant and logical given the state of security at the company. To an outsider the blunders were obvious, however, to CX employees who had become accustomed to operating in a certain manner, not knowing any other way – they seemed foreign and unfounded. This is where the training and awareness program proved its worth. By educating the users and scientist of the purpose and benefit gained by employing security, their acceptance of the changes and their willingness to cooperate with the demands of the security office increased.

### *The Facts*

Because of the compromise in the building and fire research division, the integrity of the data and the reputation of the company were on the line. Ultimately, this jeopardized the viability of CX and forced them to take a look at their overall security posture. With the long and short-term changes discussed above, CX developed and implemented a plan that would increase the overall security, while having minimal impacts on the day-to-day functioning of the company.

By involving upper management and getting their support for the actions, the implementation of the changes went smoothly. The coverage offered by both the short and long-term approaches proved beneficial to the company. The short-term fixes helped CX quickly realize the benefit of security while the long-term goals helped provide a vision for the company going forward. Passing security audits and vulnerability scans following the risk assessment removed the low-hanging fruit that would-be attackers target first. By adding a layer of defense, beyond simply having a firewall, CX notched up the level of their overall security and decreased the likelihood that a hacker would gain easy entry into their network. By increasing the difficulty of gaining unauthorized access, the hope was that attackers would move on, looking for easier targets that required less effort.

### *The Post-mortem*

Following the system compromises, an exercise was performed with the affected group to ensure that they understood the importance of securing their systems. This session was directed less at the actual immediate solution and more at the long-term goal of educating CX employees on the importance of security and changing the insecure manner in which they had been conducting business.

The major components of a risk assessment and the relationship between them were discussed in great detail. The results of this interactive conversation were put into table format, included for illustration (and distribution) below. The major assets, threats, impacts and likelihood were discussed in relation to the risks that were present. Also discussed were the recently implemented countermeasures and the mitigating impact that these had on the risks that were

determined in the previous step. The final column indicated whether or not the risk was reduced to an acceptable level, as perceived by the stakeholders in Company X. Any risk that was not at an acceptable level was added to an action plan.

| Assets | Threats | Impacts | Likelihood | Risk | Countermeasure | Acceptability |
|---|---|---|---|---|---|---|
| Data, Research Results, Lab Processes | Insider, outsider, accidental, intentional, competitor | Loss of man-hours, loss of reputation, loss of respect | High given historical track record | Data will be corrupted, manipulated, or deleted; company loses investors | Implement defense-in-depth principles, secure data | Increased to an acceptable level. |
| Scientists, Knowledge Capital | Insider, outsider, accidental, intentional | Loss of life, loss of research time | Low given historical track record | Life or job threatened | None | Increase physical security demands to make acceptable |
| Non-Networked Scientific Equipment | Insider, accidental, Intentional | Loss of man-hours, loss of research capability | High given historical track record | Adjustments /tampering jeopardizes accuracy of data | None | Increase physical security demands to make acceptable |
| Networked Computing Equipment | Insider, outsider, accidental, intentional, competitor | Loss of equipment control, computing power | High given historical track record | Machines corrupted, manipulated, or harmed; company used in other attacks | Hardened systems, removed vulnerable applications and services | Increased to an acceptable level |

This exercise was very valuable for the participants involved. It showed them a perspective that they might not have ordinarily been exposed to – that of the new security officer. It also taught them the components of determining risk in a system and the effects that mitigating efforts had on the overall outcome of the risk. Moreover, it introduced the idea of risk acceptability. The fact that risk could not always be and should not always be eliminated was a new concept for many of them. There were circumstances where risk would be accepted when the cost of fixing the risk was compared to the cost that would be incurred if an exploit were successful.

Because it is a soft measurement, likelihood was another difficult concept for participants to get a grasp on. History allowed the CX participants to claim that there are people out there that are interested in their systems and will compromise them and disrupt operations or manipulate data, given the opportunity. They realized that it was necessary to deny them the opportunity and this exercise helped show them how to get it done.

Another realization from this exercise was that the employees of CX did not have a firm

understanding of what it meant to be and operate in a secure fashion. This is not through any fault of their own, simply stated – they were not asked to look at business with that perspective in mind before. This, again, traces back to the lack of planning for security when the company was first starting out. Based on these realizations, training and awareness sessions were planned for both the short and long-term, for all divisions, and addressed these topics. People directly involved in the short-term changes needed to understand what was being done and why it was being done. This required the quick development of a session geared toward eliminating the most vulnerable elements of CX, the public network. This session was provided to the system owners and administrators as their systems were scanned. Administrators were encouraged to participate in the scanning effort with the CSO so that they might conduct their own assessments in the future.

All of the administrators that were responsible for systems in the internet-facing network, were required to fulfill at least 2 hours of training for hardening systems and reducing risk. This track was developed by the new training and awareness security support person and consisted of historical case studies from CX and other companies who suffered attacks as well as instructions on how to run commercial and freeware scanning tools. This course helped the administrators see first hand their errors as well as the benefits of operating in a secure manner.

Other courses were developed that helped address the changes that would impact the general population of employees at CX. Several of the applications that they had become accustomed to using for personal use, would now be inaccessible. For instance, file sharing and music swapping applications would have their ports blocked at the firewall and would not be in the newly developed acceptable use document and therefore against company policy. Furthermore, these employees would be taught about topics such as social engineering – one of the leading sources of private and confidential information leakage [4].

The long-term element to the training and awareness program included a plan for each group of employees of CX. This program was developed by the training and awareness analyst under the CSO. Based on a functional division of employee tasks, a series of sessions was arranged to address the most applicable situations, scenarios and decisions that would be encountered by personnel. This security program included every employee at CX from the janitorial staff to the CEO, as each had a unique realm of operation that was addressed.

## After

### *The New State*

The most immediate and most important result for Company X was a drastic decrease in system compromises. Gaining control of this element was the top priority for this security effort and was very successful. The short-term actions were instrumental in securing and locking down the public facing and historically attacked portion of the company. As a result of the steps taken to implement these security measures, a beneficial side effect was realized. There was an increase in the overall stability of the system. The raised standard for version and application requirements increased the stability of the system across the board. This relationship between stability and security will be seen throughout the changes that are implemented at CX, both short and long-term.

New state of security at CX is unrecognizable when compared to the day the Building and Fire Research division was compromised. From that day with insecure applications and services as well as unpatched and unauthorized operating systems, to today, where policies and procedures dictate applications and versions acceptable for use. It has taken time and commitment to adjust people's thinking and actions, however, the steps and persistence of the executives, security office and scientists paid off.

### *The Rewards*

A major benefit of the long-term security solution was the fact that scientists and other employees gained a set of guidelines to follow. Aside from the fact that they were mandatory, employees of CX now had a certain level of guidance from which to base their technical and business decisions. Previously, people were reinventing the wheel each time a division or group set out to do something new. Now with policies and procedures in place that govern the entire company, there is conformity in the way in which things are done. This uniformity increases the interoperability of the groups within CX and allows knowledge transfer within the company as a result of common operating procedures.

The problem facing Company X was resolved. Since the implementation of the policies and procedures and the training and awareness program, there has only been one breach of security. The breach was minor, monitored and dealt with in an efficient manner. The proceedings after the compromised occurred, involved collecting forensic data, calling the appropriate authorities and actually led to the arrest of a serial hacker. The CSO was credited in several newspapers with assisting Federal Agents in tracking down and capturing the deviant. This positive publicity increased the confidence of investors and potential investors in CX. It is also assumed that the customers of CX had an increased sense of trust in the company's secure operating procedures.

Another benefit CX realized as a result of their security program's implementation was an increase in the amount of knowledge sharing. Because the operating procedures were standard

and every division followed them, several divisions ran across common problems. These problems spurred questions and conversations that led to collective efforts and resolutions to the issues. Divisions that had previously required modem access and did not have permission to have such devices connected to the private network under the new modem policy were able to apply for an exception if they had adequate security on the system housing the modem. This system was tested by the CSO and approved. Through knowledge sharing, another division was able to maintain continuity of operations without changing their current modem-based protocol by following the example set by the first exception. The CSO now maintains a list of exceptions to the modem and other policies and periodically verifies the level of security of these systems.

### *The Obstacles*

No process is ever perfect the first time around and CX's transition to a more security-focused company was no exception. Overcoming the initial complication was crucial to the success of the transformation. This obstacle was gaining agreement and support from upper management. This was instrumental in getting cooperation from divisions and employees further down the organizational chart. Many of the executives did not see the relevance to their division. By publicizing the Building and Fire Research division's faux pas and the antics of Angry Andy, several managers saw the adoption of a security program as advantageous. For others, it was not until a series of case studies were revealed and those companies that did not assume responsibility for their own security found themselves out of business. This was the most convincing method of gaining support. While F.U.D. (fear, uncertainty, and doubt) are traditional means for selling security work, and quite effective, the recent trend has steered away from this model. Security is something that should enable a business to operate comfortably and should be desired by executives and employees – they should not be scared into security.

Additionally, there was pushback from unhappy scientists who only desired to perform research and had been happily doing so for a long time. These people who never had any problem before took the stance that "it will never happen to me." Using representatives from the Building and Fire Research division to give a testimonial stating that they used to think the same thing and after they were compromised, nearly one year's worth of data was destroyed or rendered unusable – many of the disbelievers changed their minds. Despite their large workload, small budget and resource demands they recognized that their current processes required adjustment. Although some did it begrudgingly, everyone conformed to the new regime.

Other complications associated with training and awareness typically dealt with employee apathy or over-commitment. There were several employees who were extremely busy and did not think that the training was necessary for their job function. To combat this, training line items were inserted into all employees' performance evaluations. Because the upper management at CX took security seriously, they deemed it appropriate to evaluate their people on their acceptance of this fundamental new capability. Following a memo from the CEO regarding this adjustment in performance evaluations, there were relatively few problems with employee cooperation.

Of course no single program or solution is a panacea. There will always be more and newer and better vulnerabilities. It is said, "security is a journey not a destination" [5]. Security is a constant battle. There will always be a new application exploit or Operating System vulnerability that

needs to be patched. A regularly scheduled vulnerability scanning program and up-to-date training for administrators helped CX remain ahead of the curve. Another key for CX was to eliminate the low hanging fruit and reduce their risk to an acceptable level. This was agreed upon and signed off by upper management early on and led to the creation of the short-term action items. The long-term action items speak to the never-ending process that security represents. The combination of these two proved to be very effective in getting CX to a reasonable and acceptable state of security.

By fixing the root of the problem, the amount of day-to-day fire fighting that CX's CSO and security analysts incur was greatly reduced. Simply patching the problem would have only temporarily shielded CX and it would continually be battling a problem with which they have no control and no means of enforcing.

### *The Risk*

The risk for CX went through a significant metamorphosis from being unidentified to mitigated, reduced and, in some cases, eliminated. This change was essential for CX to remain a successful company. The changes were a great investment and will serve CX far into the future. The changes required a certain amount of maintenance, but was no comparison to the effort expended had this solution not been implemented.

### *The Assistance*

The GSEC course provided the proverbial lights on the path. GSEC acted as a guide for implementing the best solution for the given situation. For example, GSEC provided broad guidance for the strategic placement of the security group to empower them to make decisions that would be respected and followed by the other divisions. GSEC also provided specific guidance such as the details on creating an effective policy requiring patches to be applied for applicable systems in a reasonable amount of time.

Overall, GSEC outlined the best practices that were applied at many, if not all, stages of the implementation of CX's security transformation. The combination of short-term and long-term agendas to effectively combat security shortcomings was derived from a series of out-of-session conversations that participants in the class had with instructors that were present during breaks and lunch. This candid advice proved to be extremely helpful and effective at CX and hopefully clients in the future.

## Conclusions

My risk assessment of the compromised web and data repository file servers uncovered long-standing, systemic problems that required a commitment by upper management to successfully mitigate the risk.

From the "10 Immutable Laws of Security", a screen saver series published by Microsoft, *Technology is not a panacea*[6] was a hard lesson for CX to learn. Their dependency and trust in the firewall and its proper administration needed to be adjusted to a more realistic view of corporate security. CX rebounded and came together as a company destined to succeed and do so in a secure manner.

### *The Approach*

The approach that was taken targeted the root of problem. This was not the quickest resolution to the immediate problem, but a combination of short and long-term actions were devised which proved to be very effective for CX. In the short term, all of the high risk, low effort fixes were implemented; this showed immediate results to management and employees and acted as a motivating agent for further security steps. The long-term action items addressed issues that were systemic in nature and were required to get to CX's ideal security posture that was laid out in the initial executive meeting. This second approach effectively planted a seed and acted as a long-term investment to improve the company overall. As a bonus, actions that began as strictly security related ended up adding value to CX's business operations outside of the security realm. Primarily, standard operating procedures helped secure the company but also led to common solutions to problems because of similar constraints.

### *The Balance*

The need for a security measures and a security program was apparent due to the break-ins that occurred at Company X. There was no doubt that if something was not done to improve the security posture of the company, that it would only be a matter of time before the company would no longer be in business. The research company could not sustain the negative publicity that was inevitably associated with a security breach.

Cost is a difficult measure to quantify in security. There is undoubtedly a way to place a value on the cost of implementing the security measure (e.g. time + materials), however, placing a dollar value on what was avoided by that action is next to impossible. There are certain intangibles that are gained when implementing a security solution, such as piece of mind and confidence. These are also difficult ideas on which to place value. Several respectable firms have done return on investment analyses on security implementations and they are promising, but no two circumstances are ever alike. As long as reasonableness does not leave the equation, security implementations derived from valid and accurate risk assessments should be sufficient. For example, $1 million should never be spent to protect a system with $1,000 but in the reverse case, a $1 million might be sufficiently protected with a $10,000 investment. Common sense should be

applied to security purchases, as in most other business related decisions. That idea was maintained in CX's security implementation.

One cost that can be tracked and trended over time is the amount of problem solving time required before and after a security solution is implemented. Overall the operating cost will typically be reduced by ending the dog tail-chasing phenomenon. Whereas if security is handled in a reactionary manner or only a short-term solution is chosen, there will be a never-ending cycle of solving one problem, only to be confronted with another. The maintenance required of CX's security group, with a well-defined security posture, is predictable and manageable. This is a much different scenario than the surprise of a system compromise and the litany of repercussions that have to be dealt with under stressful conditions. By being prepared for such an event and having a set method for dealing with them, there will be little in the way of unanticipated complications.

The security that was implemented was neither excessive nor minimal; it fit the situation and goals of Company X. The long and short-term actions complimented each other, working to achieve different things, but supporting the same overall vision for CX – a more secure computing and business environment that would enhance the ability to perform Research and Development.

The improvements in Company X's security posture helped bolster the confidence of nearly everyone involved in the process. From the scientists, to the executives to the investors, everyone walked away from the problem feeling as though the solution that was implemented was in the best interest of the company. The easily broken components of CX's façade were cleaned up and removed and the vision for the company going forward was adjusted to include security as a necessary element. In the end, Company X was successful at building a security foundation underneath an already existing structure through the various methods discussed above.

## Lessons learned

This short section contains a list of items that were learned as a result of the experience described above (and other various assignments). Some of the items seem obvious and would likely be followed in the absence of this section, yet others are a bit subtler and may be helpful to the unseasoned securitor.

**Upper management agreement** and backing is essential to the success of security efforts. This fact is especially true when implementing programs requiring a sizeable change in the habits and behaviors of the recipients of a security solution. The support of management lessens helps shoulder the unfortunate backlash that sometimes accompanies this change. This cooperation cascades through the ranks and increases the likelihood of obtaining necessary information and meeting deadlines.

**Patch early, patch often** is a phrase that was used during a GSEC class on Windows security. This adage is not only applicable to software packages originating from Redmond, Washington but all operating systems and applications that run on a system's components. Neglecting or procrastinating patching systems is a substantial cause of exploitation in many corporate systems (link here).

**Implement a regular vulnerability-scanning program** in order to ensure consistent and effective patch application and system maintenance levels. Security is no exception to the age-old *epithet* that a chain is only as strong as its weakest link. If there are components of systems that are not up to specification with regards to version or patch level, they act as a significant vulnerability to the entire system. A compromise of one component provides and entry point to other systems that would not otherwise have been vulnerable to attack.

**Security is a journey not a destination.** Security is an ongoing process. It is not a milestone or a deliverable. The IT world is constantly changing and system security must adapt to that change or it will be overtaken by it. There are several mechanisms that provide valuable information to the security community before or closely following the outbreak of a virus or the announcement of a vulnerability.

**Dedicated, security-minded people are hard to find** and hard to keep. A serious security program requires skilled professionals and they do not come cheap. Special concessions might be required in order to combat attrition in a security organization. Training, certifications and professional development are all good personnel incentives and usually have an immediate positive return on investment.

**Understanding is key**. People have a much greater acceptance rate of changes to their established routines if they understand why they are being asked to modify something that they have been doing successfully for years. New security measures often require people to alter their standard routines and without a good understanding of the justification of what they are being

asked to do there will be much more resistance to the measures. An effective training and awareness program greatly increase the likelihood of understanding and success of new programs.

**Be the voice, but not the mouth.** This lesson specifically applies to consultants and contractors. While you want to be the authoritative force behind the security recommendations that a company or organization implements, it is often better to let the orders come from someone in the company. If there is a chief security officer (CSO) or someone in a powerful technical position (CTO, CIO, etc) it is advisable to have them dictate the direction that the company is moving in – not an outsider, such as a contractor, who can be accused of not knowing what is best for the recipients. This eases the integration process significantly. This approach also helps suppress some of the dissent that would otherwise be directed at an outsider. People are less likely to criticize someone that is responsible for overseeing their boss, and them indirectly. While constructive criticism is good and welcomed, people's resistance to change can come without forethought to the benefits of what is being implemented – this is the type of reluctance that is being mitigated in this case.

## Bibliography


Associated Press. “Computer Attacks on the Rise, says FBI study.” April 08, 2002. URL: http://timesofindia.indiatimes.com/articleshow.asp?art_id=6290056 (September 1, 2002). [1]

Tripwire. “Tripwire – The Open Source Project.” URL: http://www.tripwire.org/downloads/index.php (September 1, 2002). [2]

National Security Agency. “Security Recommendation Guides” March 06, 2002. URL: http://nsa1.www.conxion.com/win2k/download.htm (April 17, 2002). [3]

Center for Internet Security (CIS). “Hardening Guides” March 06, 2002. URL: http://www.cissecurity.org/ (September 1, 2002). [3]

National Institute of Standards and Technology. “Computer Security Division” March 22, 2002. URL: http://csrc.nist.gov/it/win2k_nsa.html (September 1, 2002). [3]

CERT Incident Note. “Social Engineering.” Current. URL: http://www.cert.org/incident_notes/IN-2002-03.html (September 1, 2002). [4]

Cert Conference. “Network Security.” URL: http://www.certconf.org/presentations/1999/interintraextra/img31.htm. (September 1, 2002). [5]

Microsoft. “The Ten Immutable Laws of Security.” URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/essays/10imlaws.asp (September 1, 2002). [6]