Global Information Assurance Certification Paper

GIAC ENTERPRISES:

A Look into the Security Practices

GIAC Information Security Fundamentals+ (GISF)
Practical Assignment
Version 1.0 (July 25, 2003)

Angela K. Mello

Submitted March 17, 2004

SUMMARY

The following paper describes a fictional company, created by myself, that hired me as a full time employee under a Manager. I was assigned the tasks of reviewing all of the security elements within this company and hoped to created a more secure approach. Most of the information contained in this paper is at a high-level approach. I will take you through the process of securing a small company in an almost step by step approach for outlining what needs to be secure.

TABLE OF CONTENTS

1.) Description of GIAC Enterprises

GIAC Enterprises is an organization that helps to give children a place to play. We provide after school services to watch children in a safe environment until their parents can pick them up. We also offer full-day Daycare services for those parents who need to work and have no other place to turn. We here at GIAC Enterprises, rely on the kindness of others to keep us in business. We get contributions from many businesses and individuals all around the world totaling nearly 5 million dollars.

Keeping our website up and running is a vital part in keeping our contributions coming in. We need all those contributions each year in order to pay our 60 employees in our 4 locations nationwide and our headquarters. Our website includes an address for people to send in money in the form of checks or cash or money orders. We also have a separate page on our website for people who want to send in donations using their credit cards. We are not yet able to accept donations in the form of other currency outside of U.S. dollars.

The IT department plays a substantial role in keeping us in business. We need them to make sure that the webpage is up and running without any major problems. This webpage is our main source of income. Even having it down for a day would greatly impact the amount of contributions that we receive. We receive an enormous amount of checks and credit card payments on any given day. The amounts we receive from these sources vary on a daily basis. On average, the webpage needs to be running every day to keep our business running smoothly.

Our company has four locations throughout the United States. We have a daycare located in Southern California. This location houses just a daycare with 1 Manager and 7 employees. We have another location in New Hampshire. This location has 1 Manager and 8 employees. Another location in Michigan houses 1 Manager and ten employees. Our final location, in Iowa, is not only a daycare building, but is also our headquarters. This location has 1 Manager and seven employees working in the daycare on the first floor, and twenty-four employees working within the remainder of headquarters. Out of these 24 employees 8 are Executives and 16 are other employees.

GIAC Enterprises is a small company. We base our business on the theory that you have to spend money to make money. We spend approximately 1 million dollars for our payroll per year, which breaks down into the range of 8 – 30K depending on position. Daycare workers make as low as 8k while our IT staff make up to 30K, depending on the education range. The remaining money then gets divided between management and higher positions.

2.) Diagram and Description of GIAC Enterprises [1]

GIAC Enterprises has a network consisting of three Firewalls, two Routers, a VPN, an internal network, a screened subnet, key servers, and six switches. We chose this network set up to allow for growth within our company. This also allows us to keep greater control over who has permission to view certain information.

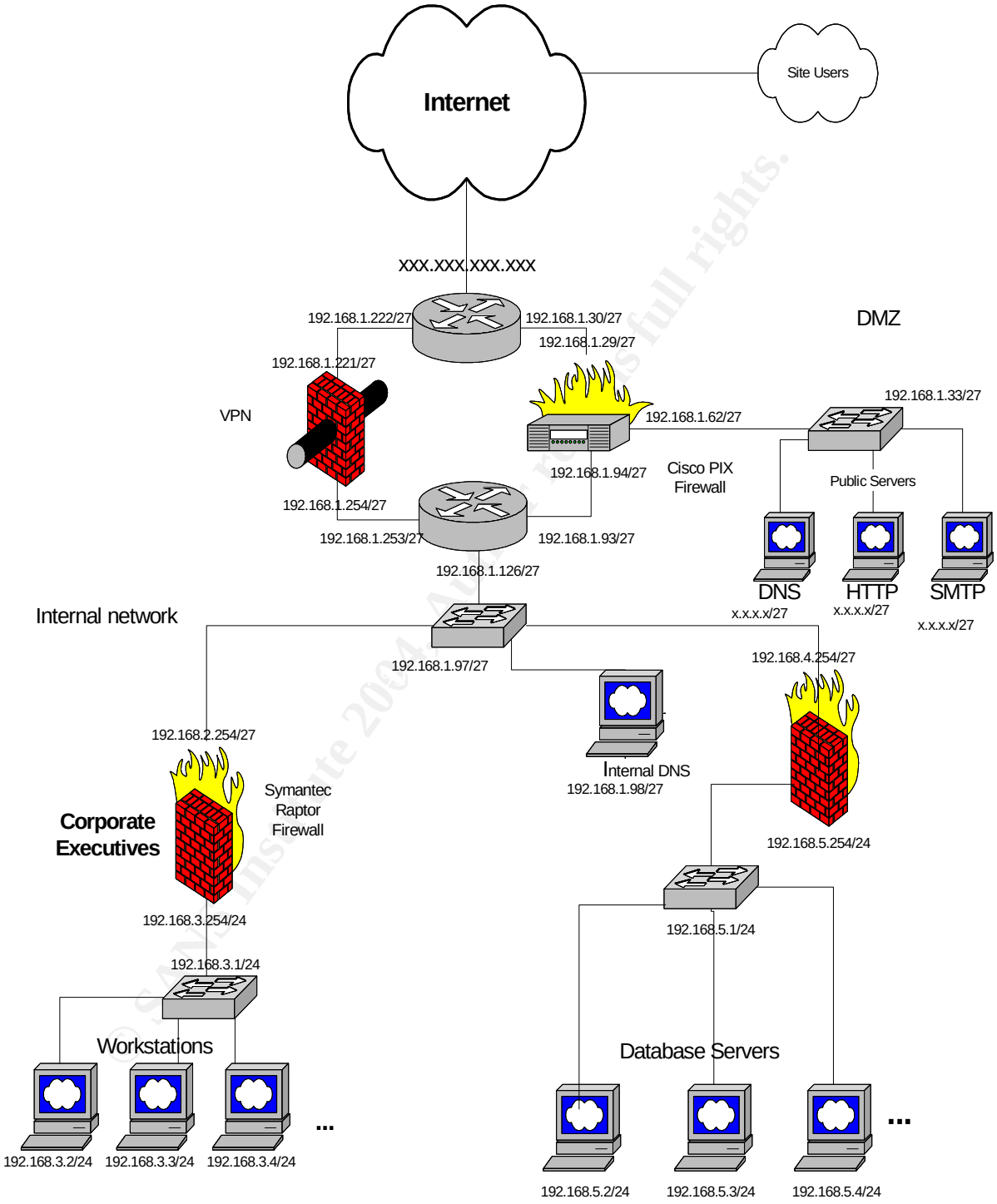
Our internal network consists of three switches and two firewalls. There is a switch at the frontline of the internal network. This allows for incoming traffic to be directed to its destination, whether that is the Corporate Executives, the internal DNS, or the database servers. Once traffic gets through the switch, if the traffic is going to either the Corporate Executives or the database servers, the traffic will run into a firewall. If the traffic is allowed by the firewall, the traffic will hit another switch to direct the information to the correct destination.

Our DMZ contains pubic servers for Web (Http), for Mail (SMTP), and for DNS. Going through the line of router to firewall to switch can only access these public servers. If a remote user who has the correct permission needs to get into the public server for any reason, they would need to first go through the router, which either sends them to the VPN or the firewall. To go to the public servers, they would be sent through the firewall, which will either allow or deny access for them. If they are permitted through the firewall, they are brought to a switch that will send them to either the DNS server or the HTTP server or the SMTP server depending on the information about the destination that was sent. If an insider wanted to access the DMZ, we would have the firewalls configured to permit their access.

All remote users wanting to access our internal network must enter our network through the VPN. This allows us to grant permissions to only those users that we want to have access.

We strive to have a complete defense in depth strategy. We have multiple methods to counter any unwanted access on many levels. This enhances our ability to continue defending ourselves even in the instance where a single item fails.

[1] Silvia, Tara. GCFW Practical, Version 1.5. March 17, 2001. URL: http://www.giac.org/practical/Tara_Silvia_GCFW.zip. I am using Tara's network design, however I modified it to better fit my company's needs.



3.) Describe your office, or department at GIAC Enterprises

We here at GIAC Enterprises strive to safely and responsibly care for all children regardless of race, creed, color, or origin of nationality.

As part of our rules and regulations, we must provide the children with toys to play with and food and beverages to consume while at our organization, in order to comply with the above-mentioned mission statement. The one thing that allows us to obtain these toys and food and beverages, the money, comes from this IT office, due to the web page. This office must secure all information regarding the webpage, customer information, employee's information, and financial information.

In my position, here at GIAC Enterprises, I report to the manager of this office. Her manager is the VP of Operations.

The IT department manages the web page and keeps it up and running constantly so that we continue to receive money from people. Of the contributions that we receive, 90% come from the web page, while the other 10% come from walk-ins or from the families of children within our program.

The IT department is responsible for and manages different assets for the company. Each of the four IT personnel has a laptop issued to them for work use and for any work related travel. The IT department is responsible for any computer related item in this company. This IT department is responsible for the following: maintaining and assuring that everyone's computers are operating with no problems, that the website is running properly, that no hackers are causing this company problems, and for helping the company run smoothly.

The IT department consists of four employees and one manager. This department is the heart and soul of this company. Without the IT department, everything would fall apart. The IT department and the total of five employees keep the other fifty-five employees continually able to do their work. We have a Finance department that handles all business related to money. This department has 1 Manager and 5 employees. Our Administration department keeps track of handling customer questions and answering phones and ordering supplies. This department has 1 Manager and 7 employees. We have daycare workers at our 4 locations that each has a Manager and between seven and ten employees. Finally we have our Executives, that consists of the President, the Vice President, the VP of Operations, the President of HR, and the President of Finance and Administration.

This IT department is situated within the headquarters building, which is located in Iowa. The expense budget for the IT department is $1,155,000. Of that amount, $155,000 is salary and up to $1,000,000 is for all equipment, maintenance, support, and training.

4.) Describe your Job Description at GIAC Enterprises

I was recently hired at GIAC Enterprises under the job title of IT staff member. This is one of the higher paying positions of this company. Everybody here must take a substantial pay-cut depending on how much money we make in any given year. My salary is right at the $30,000 per year mark. All employees at GIAC Enterprises are hired with the knowledge that on any given pay period, the amount of money we receive may be lower then we are supposed to receive. Since our business is based on the contributions that people graciously donate, we may not always have the same amount of money in our budget.

As an IT staff member, I am assigned to the IT department. I report directly to the Manager of the IT department and she reports directly to the VP of Operations. All employees other than the IT department Manager are considered an IT staff member. This enables us to spread the work around evenly and allows less of a workload to be placed on one person's shoulders. We are then able to continue our workflow even if a staff member were to leave employment.

I have been given two primary responsibilities. My first responsibility is to consistently check for any and all possible break-ins by hackers. I am responsible for testing out our security features and to check up on any new vulnerabilities. My goal is to find at least one new opportunity or vulnerability each and every day. This task is a common task among two of the IT staff members. We continually try to break into our network in hopes of finding out a new way to secure it. If a member of the IT staff were to break into our network, we would know that an outsider or an intruder would also be able to break into our network and do damage. Many people might believe that this is one way of giving an insider the opportunity to do damage to our network. However, I feel as though our network is secure and the IT staff should not be able to break in. As not all people are trustworthy, we have an auditing process. This is only done in a certain time frame and only two people have permission to do so. An executive would watch over the two individuals and keep a log containing information such as which part of the network the two individuals were working on.

My second area of responsibility is as a support person. I make sure that all the finance and administration computers, the computers at all the different sites, and the executive computers are running problem-free. Whenever one of the personal computers in the company has a problem, I am contacted by the user and may have to go to that users location to fix the problem. My daily goal for this responsibility is to fix ten problems. We strive to have each and every computer in our company continually working and to minimize downtime.

5.) How does GIAC conduct its business?

GIAC Enterprises is a fairly small company. We have Sixty Employees in a total of four locations nationwide. Mostly all of our business comes from our web page. We have a form to fill out on our site if a new customer would like to join our daycare. We have our contributions page on the web page for anyone across the world to donate money.

When we receive a request for a person to join our daycare, we first look at how many children are enrolled at that time. If we are at the maximum amount of children, we then place the child's name on our waiting list. If we have not reached the maximum number of children, then we will send a letter of acceptance to the parent letting them know that their child can start to attend. We must limit the number of children allowed because of legal and safety reasons.

Because we only get the top of the line items for our children, we have many families that would do anything to get their child or children into our organization. We are a very sought after business, similar to the top of the line schools that everyone wants to get into. We are a top of the line daycare that everyone wants their children to be a part of. People send in large donations in hope that one day their son or daughter will be able to be part of our center. We have people who are applying for their children to be a part of our center before their children are even born. We keep our waiting list this long by working as hard as we do and striving to maintain the best atmosphere and care for our children.

6.) What applications and/or what type of access are required to carry out these business operations?

GIAC Enterprises is a very simple, small company. We do not have business partners, and our customers and suppliers are limited in scale. Our customers are those who either have children enrolled in our daycare, or those that continually contribute money. Most of our communication is done by means of email. Our customers send in their contributions either from a credit card form on our web page or they can send in a check via postal mail or they have the option of walking into one of our locations and handing an employee a check or even cash. Our customers have no way of connecting to our network except to send an email or by physical access.

Our employees have more need for access than do our customers. The access our employees have is dependant upon the department they are in and the job function that they are to accomplish. These employees will only be allowed to access information on servers that they have the correct permissions. Our IT department has the responsibility of attempting to gain access to the places where they do not originally have the permission. The Finance department has access to our financial information. They need to be able to see the money that is in our bank account, and they need to be able to see who donated this money. Our Administration department needs access to our customer information. They need to be able to see if we have reached our enrollment limits at any of our locations.

Our daycare workers at our locations need to be able to connect to our network to read our company newsletter that is posted on our intranet. Any other communication that is needed from our locations should be done by means of email or the telephone. All of our locations have access to the internet by means of their own site specific ISP.

Our remote access users have very little need to access our internal network. If an IT member or a worker working at home were to need access, they would be routed through the VPN to obtain access to our internal network. If these same workers needed access to our DMZ and if they had the correct permissions, they would be routed through our firewall and a switch would send them to the correct destination address.

When they need supplies, they send an email or telephone headquarters and the employees at headquarters will place the order and have it shipped to the location. If toys are needed, we order from www.kbtoys.com, if food or beverages are needed, we order from www.peapod.com, and if general office supplies are needed, we order from www.staples.com. Of course, we must track the items we purchase and keep records of which locations have which toys and when the items were ordered. For these types of records, we use Microsoft Access.

Our business is completely under the Microsoft cloud. We use Microsoft office for day-to-day documents and presentations. We using Microsoft outlook as our email program. We use Microsoft Access as our choice for databases. We also use Microsoft Visio for our diagrams and drawings. We may add some vulnerability by going all Microsoft, but we add a great deal of user knowledge. This helps in keeping our training costs at a minimum.

7.) Identify three "crown jewels" your office has access to and is responsible for

In this company, there are certain roles and responsibilities that each area or department is in charge of. The administration department maintains the contact lists of our customers. These lists are password protected and grouped so that only the administration department can access the information. This list is stored on one of the database servers. This list is used to keep track of any and all information regarding our customer. It keeps track of the name, mailing address, child's information, etc. We allow all members of our staff to communicate with our customers; however, we limit all dealings with the contact list to only those in the Administration department. This enables us to easily audit the process.

Another vital part of our company is the information concerning our money. The finance department handles everything that deals with money. They maintain the financial information database containing all the information regarding the contributions. This database contains information regarding who donated money, how much was donated, when the money was deposited into the bank and who deposited the money. They are also in charge of making any and all purchases. If a location were to need some supplies, the location would contact the Administration department. The Administration department would take the order and bring it to the finance department for the approval that the money was there. The finance department would then record that information into the database and give the administration department the approval to place the order. This database is also password protected and only accessible by those within the finance department. This database is located on another one of the database servers.

Many of our employees, feel the most important database is for the management information such as salary, performance, background investigations, and awards for each employee of GIAC Enterprises. This is one database that the amount of people who have access is very limited. We don't want the employees to have access because we don't want them to have the option of changing any of the information. Therefore, the President of Finance and Administration as well as the President and Vice President of the company have the only access. This information is found on a removable storage device and is stored in a safe in the office. Each day, the president of Finance and Administration must take it out of the safe and work with it, or give it to either of the two people allowed access. At the end of the day, it is locked up again in the safe and behind the locked office door.

Another vital part of our success is our web page. This has gotten us where we are. We have people from all over the world who know of what we accomplish and want to help by donating money. The reputation we have earned has assisted us to attain this money that we need to run our day-to-day operations and all the purchases that we make. If someone were to tarnish what

we have built for our website, we would be ruined. It would take all of our contributions away and we would be destroyed. We need to make sure we get all the best toys and have no problems with our children getting sick from our food or hurt from our toys. We need to take care of and make sure our equipment is running smoothly. Most importantly we must strive to make our customers and employees satisfied so they will stay within our company. This information is located on our website information server which resides in the database servers area.

8.) Insider threat vector for each of your office's crown jewels

Our greatest threat to all of our crown jewels and everything we consider important comes from insiders. These insiders know the system and know who has what roles and responsibilities and who has access to what information. Our four biggest crown jewels in this company are our customer information database, our financial information database, our management information database, and our website. Each one of our crown jewels has potentially the biggest risk of threat coming from an insider, an employee. In the parts to follow, I will describe how the crown jewel might be access, and why someone might want to do so.

First, lets discuss the customer information database. This database holds the customers name, address, and phone number, number of children in our organization, the child's name, age and any and all medical history. This information is to remain private and confidential. Our customers put their trust in us to keep this information safe and secure. They do not want us selling any of their personal information to any companies. All of our employees could be potential thieves. Any one of them might take the customer information and sell it to a company wanting to advertise. This risk might be of interest to any employee because of the money one could make by selling our customers personal information.

Our financial database is another protected area in our organization. This is where we keep the information of who has donated money, how much they have donated, when the money was deposited into the bank account, and in a different section of the database, we keep information of what was purchased, when it was ordered, which location it was going to and the cost of the items. It is very important to us as an organization to keep these records in an organized way. This is an area that we pride ourselves for being so neat. The only people who are allowed access are the employees within the finance department. Limiting access, however, does not limit us from risk. An employee within the finance department may have a problem with the company and may want to see the company fail. Since they already have access to this database this would be the easiest, most realistic way for them to see the company go into very difficult times if not fail all together. If another employee wanted to harm the company this way, it would be more difficult, but not impossible. They have multiple ways that they could obtain access. They could use social engineering to get the password and logon information or they could wait and watch for a member of the department to get us from the chair and leave and open, unlocked session running. All they would have to do to make the company fail with this database would be to change some of the figures in the how much money a person donated column, in the when was the money put into the back column, or even changing any of the information of what was purchased for which location. Changing any of this information would make our smoothly running company turn into a company who can't keep track of money and who is completely

disorganized. It would take a lot of man hours to fix such a problem using our auditing process, but in the meantime our company could possible lose customers or even worse, our contributors.

Our management information database is another place for potential threats. This database includes information regarding employee name, address, phone number, salary, raise potential, promotion date and an employee rating. Any employee in the company could potentially want to change any of this information for their own benefit or to lower another employees standing in the company. This particular database is operated and controlled by the president of Finance and Administration. Those with a higher placement in the company have read-only privileges for this database. Any employee in this company could have the motivation to want to obtain access to this database. Any employee in the company might want to change their salary or give himself or herself a raise or even raise their employee rating. This database is more difficult for an employee to access. Since we limit the amount of people that have privileges to it and we store it on a removable media and lock it in a safe, an employee would need to be very creative to gain access. They would have to know the combination of the safe and the passwords to the president of Finance and Administrations computer. This is no easy task, but it is possible for someone who needs it enough. All they would have to do is to try to use Social Engineering to get the passwords for the computer and they could just wait around and watch when the safe was opened in order to obtain the combination for the safe.

Our most crucial crown jewels for the company success is our web page. Having this up and running allows us to receive contributions from all over the world and it allows us to get our name out to people who wouldn't have otherwise heard of us. The more notoriety that we get, the more contributions we are able to receive, which keeps us in business. Any employee within this company could possible be a threat. Anyone who wants to see the company fail or run into a lot of financial difficulties would have the motivation to damage or alter our web page. The members of the IT department have the easiest access to the information since they already have the passwords and the knowledge to do some damage. The rest of the staff could either hack into the web page from home or an alternate location or could obtain the password from some member of the IT department and access the information easier.

9.) Outsider threat vector for one of your office's crown jewels

Outsiders to this company are also a major threat risk. We feel as though outsiders, those who do not work for this company, might still want to do the company harm. We also must be aware of ex-employees looking for revenge.

We see their greatest chance of causing disarray in the company is through our web page. One could use password-cracking programs to hack into the web page information to change any of the information within. This would not only damage our web page, but it would also damage our trust with our customers. We need to keep everything at least appearing to run smoothly.

There are a million reasons why a person might want to hack into a web page. A person might just be playing games and not understand the full damage being caused by their actions. A person might truly be out to harm our company for the purpose of causing our company to go under. An individual may just be looking around, learning about how to do new tricks. They might not be looking to do damage to a site. It is the simplest little actions that might cause the biggest damage.

To make this company go under, one would need to alter information on our web page with the target being the contributions page. A person could cause a great deal of damage by changing the address to which the check or cash was being sent. This would bring our company to a complete standstill. A person could change the name and address of whom to send the money to and put in its place their name and address and they would make a great deal of money for themselves. A person could just change a word or a number in our telephone and we would lose our customers.

10.) Malicious code threat vector for one of your office's crown jewels[2]

Malicious code is a serious threat for any business that is connected to the Internet. IT departments face the most difficult challenge of trying to stay on top of all new variants of malicious code, as well as worms and Trojans. The only known methods of fighting malicious code is through education and through keeping up to date on antivirus signatures. However, even the best IT personnel can be caught off guard by a new variant.

W32/ Sober.d@MM is one of those variants. This particular worm is a variant from the W32/Sober.c@MM worm, which are both mass-mailers that propagate through email. This worm contains its own SMTP engine and adds values in the registry to run itself as the system starts. This worm affects Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, and Windows XP systems. This worm does not affect DOS, Linux, Macintosh, OS/2, Unix, and Windows 3.x systems. This worm, if not removed, allows access to your PC by hackers or viruses.

This worm spreads itself to email address found on your computer. It claims to contain a patch from Microsoft for the W32/Mydoom@MM virus. The emails body is either written in German or English and contains an attachment of either an .EXE or a .zip file.

This worm could potentially cause harm to GIAC Enterprises because of the nature of the worm and the afflictions to our customers. Our company depends on loyalty from our customers. We keep a database of customer information, which contains many email addresses. These email address allow the worm to propagate itself to all of our customers with email addresses. This produces a greater risk of losing customers and losing contributions. Not only are our customers and contributions affected, but out computer system itself is affected. Because this worm runs itself when Windows starts. This worm also affects our computing resources by having an additional process running and sending emails when starting up. One last area where this worm affects GIAC Enterprises is with Employee time and workload. This worm will need to be removed from all of our computers that were affected, but all the computers must be checked. This will take time away from other jobs that need to be completed and add additional cost for travel expenses that would not have been there otherwise.

[2] Symantec Security Response. W32.Sober.D@mm. URL: http://securityresponse.symantec.com/avcenter/venc/data/w32.sober.d@mm.html, Network Associates URL: http://vil.nai.com/vil/content/v_101081.htm, What You Should Know About the Mydoom and Doomjuice Worm Variants. Published: January 27, 2004. URL: http://www.microsoft.com/security/antivirus/mydoom.asp

11.) Identify the most severe threat

Our most severe threat to GIAC Enterprises comes from insiders. Insider threat has potential risk to the most important aspects of our security, the confidentiality, availability, and integrity or our crown jewels.

This threat is the most severe threat because it has the greatest likelyhood of occurring. Whether it is from an employee just looking around our company files, or from an employee knowingly causing harm to our business workflow.

If an insider were to cause harm to our workflow, there might be a great deal of damage that was done. If an employee were to alter something within our customer information database different things might occur. If we notice the change right away, we can just fix it and no damage has been done. If we don't notice it for a while, the risk of a higher degree of damage increases. We could potentially lose a customer or a group of customers and perhaps miss-out on some contributions we would have otherwise received.

If an employee were to alter something in our financial information database, as soon as the change was noticed it would be fixed, and if we knew who placed the change, we would need to find out why the change was made. We would need to find out if the change was made in error or if the change was done on purpose. Any changes to this database could potentially result in loss of money, loss of checks, and loss of contributors, which could destroy our business.

If an employee were to gain access to the management information database and make changes to either their salary or another employee's salary, than once noticed, it would be returned to its previous value and if we could catch the employee who made the change, they would be fired. If we don't catch these changes soon enough, the difference in salary amount could potentially leave us no money for supplies for our children, which could cause us to lose business and possibly destroy our business.

If an employee were to add destructive content to our website, we would be destroyed. We use our website to get our name out and to get people to send in contributions. The majority of our contributions come from people all over the world who have seen our website. If changes were made to our address page or our credit card page, we would be in a great deal of trouble until the change had been noticed. This is where we get 90% of our contributions.

If while auditing, we find the person responsible, immediate action would be taken and the employee would be fired.

12.) Recommend a remediation strategy for one of the threat vectors you have described [3]

GIAC Enterprises is a fairly new company that is still growing and always learning. While discussions about the threats and severity have been ongoing, discussions covering the topic of a remediation strategy have begun to take focus. The remediation strategy for GIAC Enterprises includes topics such as creating a security policy that is written down, implementing patch management and antivirus updates, instituting an employee training program, and maintaining a vulnerability assessment product.

Our remediation strategy is a phased strategy. The first phase that we must implement is writing down a living security policy. This will need to be updates on a determined schedule written within the document itself. Our security policy needs to include details on Priority, Value, Costs, Time, and Limitations. In this policy, we need to think about the topics of Protection within the organization, the responsibility for maintaining security, Password Rules, Antivirus Rules, Protection from the inside out and Protection from the outside in.

The next phase in our remediation strategy deals with implementing antivirus updates and patch management solutions. In this phase, we need to analyze our current solutions to update antivirus signatures and managing all of our patches. We need to take a look at the current standards and implement ways to reach the same level if not exceed with a better approach. Our signatures need to go out to all of our sites as soon as possible in order to keep current signatures to fight the latest and newest viruses or malicious code.

The third phase in our remediation strategy is to purchase and maintain a vulnerability assessment program. This program needs to obtain a product that will scan all of our workstations and servers and access where our vulnerabilities are located within our system. Then we need to take the appropriate steps necessary to ensure that we are no longer vulnerable to that particular area.

The final phase in our remediation strategy involves starting an ongoing employee-training program. This program needs to educate our employees about insider threat, outsider threat, our ethics policies and other problem areas. When we have an employee who is educated about why looking into other employees' files is wrong and possibly a cause for termination of employment, then our employees should feel less likely to want to attempt this action.

This remediation strategy will not be completed overnight. This will be an ongoing approach. We are estimating that the first phase of this strategy, the security policy, will take from 6 months up to 1 year to complete. This timeframe will cover the following steps:

---

[3] The Basics of Securing Your Business Network. URL: Support.3com.com/training/3comu/courses/content/small_business/security_basics/main.htm

- Assess Risk
- Determine Vulnerability
- Analyze Budget
- Write Security Policy
- Implement Security Policy
- Continually Audit Security

These 6 Steps are gong to need to be checked and updated according to the time written into the security policy document itself.

The second phase of the remediation strategy will not take as long as writing the security policy. The estimated timeframe for completing is expected to be approximately three months. This time will include analyzing our current approach, understanding the current standards and the implementation of the newly decided upon approach.

The third phase in the remediation strategy, the vulnerability assessment, should also not take any longer than the estimated timeframe of the second phase. The estimated timeframe for phase III is approximately three months or less.

The final phase in our remediation strategy, the educational training program, is an ongoing program. We hope to be able to offer classes when needed. This program should be updated at least once per year.

The entire strategy should be in place and running in anywhere from 1 year up till 18 months.

The total cost of implementing this strategy will be no more than $25,000. Being that we are a non-profit organization, we would get our products at a discounted price. This will include the resources needed, employee time and the items purchased. The VP of Operations should write the security policy with help from the IT department manager, the President, and the Vice President. This is going to take a lot of employee time and effort put into this instead of other projects. We would need to spend money to purchase a patch management product and a vulnerability assessment tool. We expect this whole strategy to cost no more than $10,000. We are not including employee time or pay because their pay is determined by how much money we receive in contributions. The $10,000 breaks down to include cost of patch management tool and the vulnerability assessment tool, licensing costs, and maintenance costs. It will not include the cost for hiring a speaker to come and present information to our employees. This cost is not going to be associated with the implementation, this is a cost issued at the time when a class is necessary.

13.) Review the backup strategy [4]

I have been assigned the task of assessing our back-up strategy for data stored on personal work computers. Our current strategy involves backing up only the data on our networked drives. This would be a great approach for our employees to store all their files on the networked drive and then only backup that one drive for all employees. However, this policy has never been enforced and since habits are difficult to break, a new plan must be devised.

I have come up with a solution that should work for our small company. I have taken a close look at what information is stored on each department's computers. Our remote sites do not need to be backed-up. These computers are mostly used for email and web browsing. We need to concentrate our efforts on computers within the main headquarters, where we have our corporate executive computers, our IT department computers, our HR department computers, and our Finance and Administration department computers.

Many options were considered. We considered connecting to each computer with a USB port and a portable zip drive, having the IT department running around after hours backing up each computer, having each individual person doing their own backups and buying an automated backup product. We finally decided upon having each employee do his or her own backups.

We decided on this choice for a number of reasons. First, our IT department is very busy. They do not have the time to be able to go around to each employee's computers and do the backups. Secondly, we could hold a two-hour training session and walk all of our employees through the step-by-step process of doing a simple back-up all at the same time. This would ensure that all of our employees understand how to do the backup and help to control the arising problems for the IT staff. Thirdly, we can keep the cost down by using inexpensive storage media.

We will be doing a very simple back-up procedure for all data on individual employees computers. Each employee will be handed a rewrite able CD from their higher-up on the 20th of every month. When the CD is received, this will be a sign for the employee to go and copy all the files in their My Documents folder to the CD. The CD then needs to be handed to the IT department Manager before the end of the day. The IT department managers job is to inspect the CD and make sure the employee actually made the backup and then the CDs must be stored in the restrictive access storage room behind a locked door.

[4] Staples Catalog 2003

Implementing this strategy assures that the back-ups are completed and that nothing is wasted. We have no need for any additional software products. Since all of our computers already have a rewrite able CD-RW drive, we do not need to purchase any additional hardware. The only thing that we need to purchase is the CD-RW's. If we have 12 back-up sessions, one per month, per year, per employee, this would total at most 24 employees * 12 CD-RW's, which totals 248 CD-RW's per year. If we purchase 5 of the 50 CD-RW's from Staples that would total 250 CD-RW's at a cost of $190. As mentioned before, employee pay is based on the contributions that we receive. The total cost for implementing this strategy for backing-up data on individual employees computers would be approximately $200 per year.

These CD-RW's will be stored in a locked storage room. This room is a restricted access only room, and the only people allowed in are the IT department manager and the VP and President of the company. By limiting the number of people who have access, we significantly lower the risk of someone getting their hands on this information. This room has a card only access, and only the individuals listed about have the code on their card to allow them access. These CD-RW's are each stored in a CD case with a cover and a label on each. We will keep a back up for at least 3 months, but no longer than 6 months. This will keep the amount of CD-RW's that we need to continually purchase to a minimum. After the 6 months have come, the CD-RW will be overwritten with a new months back up.

14.) Review offsite backups

Along with the simple back-up strategy that I just explained, we also have an enterprise solution that backs-up all of our database servers. These are all stored together in the same locked room. But what happens if there is a fire or another kind of destruction element that happens in this building? A plan must be devised in that case. We need a way for the back-ups to be stored off-site.

I have devised a plan to store copies of our back-ups at an offsite location. We have locations spread throughout the US, but if we stored our back-ups in one of our remote sites, it would take a longer than acceptable length of time to get them to and from storage. We need a location that is outside of our building but in close proximity and will be a safe location for our storage media. We also must consider the charge for such a storage facility.

Since storing out back-ups at one of our remote sites is not an option, we figured our best approach would be storing our back-ups in the town bank. There we would have the security of having a safety deposit box that was locked up and stored in a fire resistant metal box.

Having our back-ups in the local bank gives us many benefits. We can receive a reduction of the cost of the safety deposit box. Because we are a local business in the childcare industry and with the bank knowledgeable about how we receive our contributions, the bank can give us a significant reduction in the normal fee. We also should be given a discount because we will be making our deposits in this bank and keeping all of our financial investments contained with this bank. We could become a very loyal customer to this bank.

Our plan would break down in the following way. Each month on third Wednesday, the IT department manager will receive all employees' back-ups and all the back-ups for the servers. Since we have already purchased the initial 250 CD-RW's for the first year in the supplemental back-up plan, we can use half of the purchased CD-RW's as back-ups and the other half as the copies. The day after the IT manager receives the employees and server back-ups, they can begin to make copies of all the back-up CD-RW's and label and date all of the copies. The IT manager will then take the copies to the bank and make the deposit. Since we should be able to store 700 MB of data on the CD-RW, we can use the same CD-RW's for a few months. This means the IT manager will need to withdraw the CD-RW's from the bank the day before the back-ups to bring the CD-RW's back to the office.

We will have most of the initial tasks already completed during the revised supplemental back-up plan. We will have already purchased the CD-RW's so the only step we need to complete at this point is to go to the bank and open up a safety deposit box and discuss the terms and conditions along with the fees for having this safety deposit box. After that is completed, we need to inform the IT department manager of the new duties that they will be tasked to complete every month.

After the initial steps, we need to put the plan into action. This will involve making sure the IT manager receives the first set of employee and server back-up CD-RW's and that the manager makes the first set of copies. The IT manager must also label all the back-up copies in the same way that the original back-ups are labeled, with the name of the employee, and the date. The back-up copies must also have the word "copy" written on the top of the label. This will let the IT manager know which CD-RW's go to the bank and which CD-RW's go into the locked storage room.

We here at GIAC Enterprises pride ourselves in our confidentiality safeguards. By storing our backups in a locked storage room with restricted access, we ensure that only those employees who need access have access. Confidentiality for us, means knowing that only those that need to see the data, see the data. We are keeping our confidentiality safe by storing our back-up copies in the bank. By using the bank as our offsite storage location, we limit access to only those who have the key, and this is limited to just the IT manager.

What are we going to do to safeguard the integrity of the data? Having the back-ups stored in the restrictive access locked storage room, we limit access to only those who need access. By having limited access we ensure that nobody changes or alters any of the data. By storing the copies in the bank, we are also ensuring the integrity of our data because we only allow the IT manager to make deposits to the bank or remove the copies from the bank. This ensures that only the IT manager has access to the copies from before they are made until they are deposited into the bank.

With this plan, our information will be available when we need them. The bank is the safest place I know. People have tried to use explosive devices to break into a bank but most fail. This means that in a natural disaster of many kinds, the bank will still be standing and our data will still be available. If we need to get a hold of our back-up copies, the bank is just a short drive away. We will have our back-up copies within a half-hour of when we first ran into a problem.

How do we know that this plan will work? We will audit our process. Each time a person enters the restricted access storage room, we will have them enter their name, what they removed, how long the item was in their possession and the purpose for the removal. We know that the only person allowed to be in possession of these back-ups is the IT department manager. The manager should only have the CD-RW's on the third Wednesday of each month and the Thursday after. Any time other than that would be under suspicion and the manager would be questioned. With our back-up copies at the bank, our access is again limited to only the IT manager. A log will be kept for the bank deposits and withdrawals for the safety deposit box. There should be no withdrawals at any other time other than the third Tuesday of the month and there should be no deposits other than the third Thursday of the month. Again, if anything differs from this set-up, the IT manager will be questioned. If we run into any problems with our reloading of the back-ups, the IT manager will be questioned and possibly terminated from the company.

15.) Devise a guerilla business continuity plan [5]

GIAC Enterprises is in need of a business continuity plan. After reviewing our current approach, I feel as though we need to start over from step 1 again to dramatically improve upon what we have. We need to have a business continuity plan that will allow GIAC Enterprises to pull through and continue on with business after a disaster.

The most important step we need to take before we begin our process is to get support and backing from the President and Vice President of the company. By having them understand the purpose of why we need a business continuity plan, we ensure that when the project is completed, it will not fail. We also ensure that we can get a hold of the resources that we need and any help that we are in need of.

Now, we are ready to begin planning. The steps we must follow are Identify assets, What threatens those assets, How can we protect and recover those assets, Document the results, test and review and finally provide training and raise awareness[1]. We have already completed identifying the assets, answering what threatens the assets and answering how we protect and recover those assets. Our assets are our customer information, our management information, our financial information, and our web page information. We are at risk of damage to these assets from employees within the company, people outside the company, disgruntled ex-employees, and natural disasters. We protect our information by protecting the confidentiality, availability, and integrity of the information.

We must now document the results. It will be broken down into six selections, an Introduction, Crisis-management structure, locations, procedures, exercise log, and a revision history. We are developing a guerilla business continuity plan, which means concentrating on only 1 percent of the possible disasters.

Introduction: A business continuity plan details the steps to follow to continue with everyday business functions as normal as possible in case of a natural disaster or any other kind of disaster. This plan will cover what do to if our headquarters building is rendered un-useable from a fire or a hurricane like disaster. We will need to have the support of our entire staff at headquarters and the must all be knowledgeable about the actions necessary.

Crisis-Management Structure: The President and Vice President are our executive team. They will be in charge of putting our plan into action. They must be notified in an emergency and they must evaluate the situation. Our management team includes the VP of Operations, the President of HR, and the President of Finance and Administration. They are in charge of assessing the safety of all out employees and calling the appropriate emergency response personnel. Our company's response team includes the Manager of the IT

[5] SANS. Track 9 – SANS Security +S, 9.6 Security Start to Finish. 2003.

department, the Manager of Finance, and the Manger of Administration along with all of our remote site employees. They will be in charge of setting up our alternate site as quickly as possible. The IT Manager will need to get the back-up copies from the bank and bring them to the new location.

Locations: Our command center is our headquarters building until it is rendered un-useful. If this location is rendered un-useful, our command center would then be moved to the nearest structurally safe hotel.

Procedures:

1. Incident is Discovered
2. Executive Team is notified
3. Management team assesses safety of employees
4. Emergency Personnel contacted (Police, Fire, etc)
5. All employees telephoned to help
6. Hotel Conference Room located
7. IT Manger gets back-up copies
8. New location set up
9. Business returns to operational

Exercise Log: This will need to be completed after plan is put into effect. This should include details on the tests that were run and the results compiled.

Revision History: This needs to be completed after plan is put into effect. This should include details on when this document was revised and by whom.

In order for this plan to begin, we need to do some initial tasks. We need to compile a phone list for all employees to be notified at time of the emergency. We need to compile a list of nearby structurally safe hotels with available conference rooms. All employees must be informed of their part in the process and training or testing sessions must be set-up.

After the initial steps are completed, we only have a few tasks that need to be done repeatedly. We must revise the phone list to make sure we can get a hold of all of our current employees. We also need to revise our Continuity Plan to ensure it works for our growing business.

In order to make sure that this approach works, we need to do periodic testing. Our executive team will oversee the tests and evaluate how well the plan worked.

The IT department can use this approach for all of their operations. They need to devise a plan that will cover what happens if a virus destroys one of our server, or other interruptible problems. They will need to follow an outlined plan in order to regain normal business flow as quickly as possible.

This is also a good approach for GIAC Enterprises as a whole. Having a documented procedure for different problematic situations take much of the confusion and denial out of the foreground and put the plan in the minds of all the employees.

LIST OF REFERENCES:

1.) Silvia, Tara. GCFW Practical, Version 1.5. March 17, 2001. URL: http://www.giac.org/practical/Tara_Silvia_GCFW.zip.

2.) The Basics of Securing Your Business Network. URL: Support.3com.com/training/3comu/courses/content/small_business/security_basics/main.htm

3.) What You Should Know About the Mydoom and Doomjuice Worm Variants. Published: January 27, 2004. URL: http://www.microsoft.com/security/antivirus/mydoom.asp

4.) Network Associates URL: http://vil.nai.com/vil/content/v_101081.htm

5.) Symantec Security Response. W32.Sober.D@mm. URL: http://securityresponse.symantec.com/avcenter/venc/data/w32.sober.d@mm.html

6.) SANS. Track 9 – SANS Security +S, 9.6 Security Start to Finish. 2003.

7.) Staples Catalog 2003

Last Updated: July 26th, 2017

Upcoming Training

Security Awareness Summit & Training 2017	**Nashville, TN**	**Jul 31, 2017 - Aug 09, 2017**	**Live Event**
SANS San Antonio 2017	**San Antonio, TX**	**Aug 06, 2017 - Aug 11, 2017**	**Live Event**
SANS New York City 2017	**New York City, NY**	**Aug 14, 2017 - Aug 19, 2017**	**Live Event**
SANS Chicago 2017	**Chicago, IL**	**Aug 21, 2017 - Aug 26, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
Community SANS Portland SEC301	**Portland, OR**	**Sep 18, 2017 - Sep 22, 2017**	**Community SANS**
SANS Baltimore Fall 2017	**Baltimore, MD**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
Community SANS Cupertino SEC301	**Cupertino, CA**	**Oct 02, 2017 - Oct 06, 2017**	**Community SANS**
Community SANS Toronto SEC301	**Toronto, ON**	**Oct 02, 2017 - Oct 06, 2017**	**Community SANS**
SANS Phoenix-Mesa 2017	**Mesa, AZ**	**Oct 09, 2017 - Oct 14, 2017**	**Live Event**
SANS Tysons Corner Fall 2017	**McLean, VA**	**Oct 14, 2017 - Oct 21, 2017**	**Live Event**
Community SANS Boston SEC301	**Boston, MA**	**Nov 06, 2017 - Nov 11, 2017**	**Community SANS**
SANS Miami 2017	**Miami, FL**	**Nov 06, 2017 - Nov 11, 2017**	**Live Event**
Communtiy SANS Chantilly SEC301	**Chantilly, VA**	**Nov 13, 2017 - Nov 17, 2017**	**Community SANS**
SANS London November 2017	**London, United Kingdom**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
Community SANS Houston SEC301	**Houston, TX**	**Dec 04, 2017 - Dec 08, 2017**	**Community SANS**
SANS Cyber Defense Initiative 2017	**Washington, DC**	**Dec 12, 2017 - Dec 19, 2017**	**Live Event**
SANS Security East 2018	**New Orleans, LA**	**Jan 08, 2018 - Jan 13, 2018**	**Live Event**
SANS Las Vegas 2018	**Las Vegas, NV**	**Jan 28, 2018 - Feb 02, 2018**	**Live Event**
SANS Southern California- Anaheim 2018	**Anaheim, CA**	**Feb 12, 2018 - Feb 17, 2018**	**Live Event**
SANS New York City Winter 2018	**New York, NY**	**Feb 26, 2018 - Mar 03, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**