Global Information Assurance Certification Paper

Paul R. Rosenquist

Submitted September 7, 2004

GISF Practical Assignment:
GIAC Aircraft Manufacturing Corporation

Practical Assignment Version 1.0

Summary:

The contents of this paper will discuss an overall view of a fictitious company called GIAC Aircraft manufacturing and the part I play in it. At the beginning, we will review the general background of the corporation as a whole. This will include what they do and how they do it. We will then go into a more specific area that I am a part of. That being information security. We will discuss how they currently stand from a network and security point of view and some issues and risks that exist. We will then go into some possible remedies for some of these issues. In the end, we will recommend backup and business continuity solutions.

1) Description of GIAC Enterprises

GIAC Enterprises is an aircraft designing and manufacturing company. We have three main lines of product. They include private, medium sized commercial and military transport aircraft. The original company was established in Racine, Wisconsin USA in 1967. GIAC started with one main building and the only product produced was mid sized commercial aircraft. In 1983, GIAC began designing and building military transport aircraft. In 1994, GIAC purchased a private aircraft designing and manufacturing company located in Florida. Finally, in 1999, GIAC purchased a commercial aircraft building company located in Germany. In addition to those three main location, there are 14 parts distribution centers around the world. Ten are located in the United States and four are located in Europe,

There are a total of 3,000 employees corporate wide. 1500 are at the original main location, 800 in Florida, 500 in Germany, and about 10 - 15 employees at each parts distribution center. The total revenue corporate wide is approximately 3 billion dollars annually. Approximately 20% of which is from parts sales.

Payroll costs are approximately $126,000,000 per year. The average salary range is $25,000 - $35,000 per year,

The role IT plays in earning revenue is that we leverage our business expertise and technology to contribute to the company's overall performance and growth. In other words, we establish and maintain systems in a secure and stable manner in order to maintain the day to day operations and provide future development corporate wide.

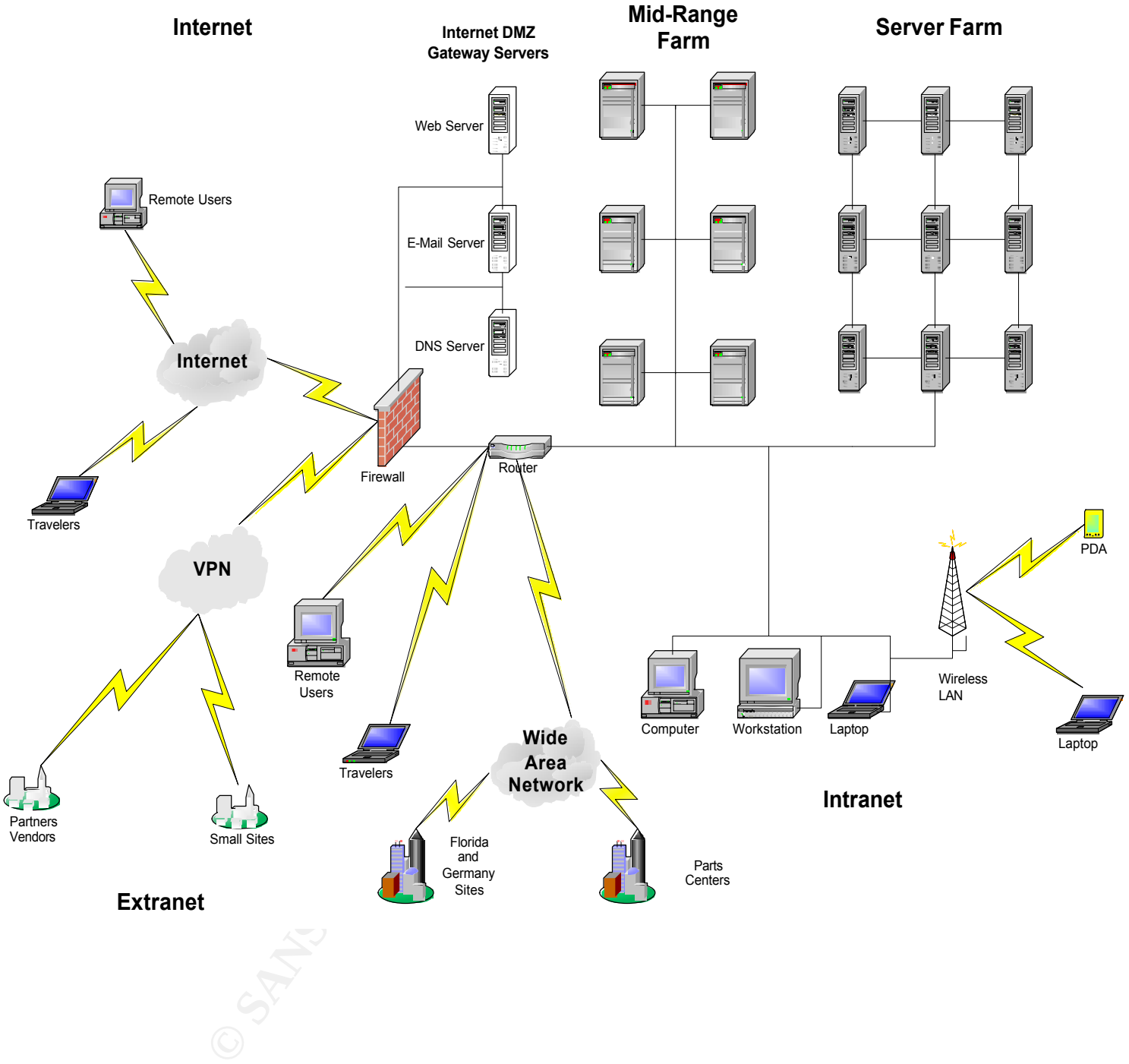
There is a Corporate Help Desk, Network team, and Operations team located within the main Racine location. The Data Center houses the main servers, systems, firewall, etc. The main corporate facility also has a company based PC Services team, Applications team, and Network team. The Corporate Help Desk is the primary location that all locations contact for issues. The Florida and Germany locations each have there own PC Services team, Applications team, and Network team. If needed, the Corporate Help Desk escalates tickets to the Corporate (third level) or local support teams. Each parts center has two to three "Super Users". These "Super Users" have more technical knowledge and training than a usual user and are able to troubleshoot many issues that occur locally. A better description of all the team and user roles will be discussed later.

2) Diagram and Description of GIAC Enterprises

GIAC has a fairly simple network design with standard security features and user requirements. The main servers, router, and firewall are located at the

corporate data center in Racine. There is one managed firewall. A router is connected internally to the firewall. The router is the main point that connects the internal servers, user workstations, wireless LANs, and wide area network (service centers, remote business sites), and some remote users and travelers. In addition to that, the internet, DMZ, and VPN are connected to the firewall externally. VPN is used for some of the smaller sites, and vendors. A Citrix Secured Gateway[1] is used for travelers, home users, and various wireless devices. At this time, no intrusion detection systems are in place. AS400's, UNIX boxes, file and print servers, application servers, and database servers or located on the internal network. There is an e-mail server, DNS server, and web server on the DMZ.

GIAC NETWORK DIAGRAM



3) Description of my office, or department at GIAC Enterprises

I work at the corporate location and I am part of the corporate architecture group. My department consists of four team members and a team manager. My title is Corporate Security Architect. The other position titles in my group are Corporate Network Architect, Corporate Telecommunications Architect, and Corporate Systems Architect.

My position is responsible for making recommendations and implementation of policies and products related to IT security. The other three architects in my

area have similar responsibilities for different areas. Telecommunications involves all forms of communication from cell phones, to desk phones, to PDA's, to calling cards. Network includes anything related to network connections internally and externally. Systems includes applications and servers. Our group manager's title is Director of IT Infrastructure and he reports directly to the Vice President of IT.
Our main function as a team is to manage the corporate systems as a whole. Each location has their own needs and designs, but with all locations and companies needing to communicate and share information, the need for a group that oversees how everything comes together is obvious. That is where we come in. We architect standards, systems, policies, and procedures that intertwine all IT functions corporate wide. Also, we manage vendors and contracts that touch all locations. These functions are in our hands simply for cost savings and organization. For example, it makes more sense to have a cell phone plan that is corporate wide. By increasing the volume of cell phones under one contract, better rates can be applied. If each company had their own cell plan, they would individually be paying more than if the cell phones for all companies fall under one contract. In addition, compatibility becomes less of an issue when all locations use the same vendor and equipment. It would be difficult for one location to manage this type of situation for all locations, so it falls under the Corporate Architecture group.
The vision of the Corporate Architect Group is to provide the strategic business units the services and support to accomplish business objectives quickly and decisively, while seizing market opportunities. We expect to do this by providing the needed services and support through shared services and distributed IS support models, reducing the technology footprint, and improving the system stability to reduce the cost of services, increase the quality of services, and reduce the time of delivery for these services.
Each member of our office has a laptop, cell phone, pager, and PDA. Each of our areas (Telecommunications, Network, Security, and Systems) has servers and different equipment for testing. Security for instance, has wireless equipment for testing, servers for testing IDS systems, vulnerability scanning, etc. Telecommunications has cell phones, PDA's, etc. for testing and reviewing. It is our group's responsibility to be up on technology and standards in order to make recommendations for corporate wide distribution and implementation.
Our group's budget is $900,000 per year. $300,000 is for our five salaries and $600,000 is for training, development, testing, and outside resources. This is in comparison to the $3 billion earned annually by GIAC. GIAC has 3000 employees overall.

4) My job description at GIAC Enterprises

My job title is Corporate Security Architect. My salary is $45,000 per year.
The office I am assigned to is the Corporate Architect team.
My manager's title is Corporate Director of Infrastructure.
My primary job responsibility is creating the policies and procedures for

corporate IT security. This involves researching products and policies related to IT Security. Things like wireless technologies, authentication, authorization, encryption, auditing, and monitoring. I research these items and develop policies and procedures to go along with them. I then present recommendations to my manager, the individual division directors of IT, and the Vice President of IT. When it is decided that a specific item or policy is needed or acceptable, I aid in the implementation of that item or policy. This is a very difficult area to measure. Based on industry standards, I am able to show where we are at and future steps that are needed. I am reviewed every six months as to what recommendations and implementations are successful and what ones are not successful. I can review and present "what could have happened" if we had not implemented an item and base an increase or decrease in profits upon that.

My second primary responsibility is monitoring and auditing. Each division is responsible for following corporate policies which may include auditing and monitoring. However, I am responsible to make sure that all divisions and locations are following these corporate requirements. I do random vulnerability scanning of wireless and wired networks. I audit the authentication and authorization process the locations are using. I do penetration and vulnerability testing of new and current servers, equipment, PC's, etc. The measure of success for this area is by reporting. I organize and distribute my finding and audits concerning the security level of all our locations. I present these findings to my manager and I make recommendations concerning them. He then distributes them to the individual directors and Vice Presidents for review.

5) How does GIAC conduct its business?

Many of the products GIAC produces and sells are designed by engineers employed by GIAC. These designs are created based on market and customer needs. GIAC has standard product lines that can be modified to the customer's wishes as needed. Our products are advertised and orders come in through a sales team. All parts required are stored in warehouses onsite at each location and get reordered when they get below a certain limit. Once an order has been finalized, production begins. Once the product is completed, the customer is billed. After the bill has been satisfied, the product is delivered. There are different warranty packages that can be purchased on new and rebuilt items. If replacement parts or accessories are needed, they can be purchased or obtained from a parts distribution center.

As stated earlier, orders come in through a sales team. The sales team can receive and process an order several different ways. It can be done through e-mail, phone conversation, on-line, or in person. Sometimes all of those methods are used with one order. These orders are processed on an AS400 system. Costs, parts, adjustments, and timelines are all processed through this system. The contracts are created, approved, and signed. The requirements are automatically distributed to the factory and parts are automatically ordered or replenished as needed. Production begins in the factory and all steps and

stages are recorded. Once the product is completed, billing is automatically generated through the AS400 system and the product is tested and ready for delivery. Every step of the process is recorded and saved on the AS400 for future reference. Once the billing is completed and the payment is satisfied, the product is delivered. At that point, all information concerning the product and its warranty are saved.

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

There are several different groups of individuals that need to access the GIAC network. Each group may have different or similar needs for access. It should be noted that all GIAC employees (corporate wide) are provided with a unique user ID through the human resources department. If they require network or system access, they must complete and submit an access request form and it must be approved by the proper individual(s) before access is granted. System access is always based on job description and need. For the purpose of this exercise, we are going to break it down into five different groups.
They are office staff, sales staff, shop staff, vendors, and customers.

The office staff consists of executives, finance, accounts payable, accounts receivable, human resources, engineering, IT, parts distribution, etc. Racine, Florida, Germany, and the parts distribution centers each have what we consider office staff. All of the staff at these locations must communicate with each other. So they are all wired together through the corporate location in Racine. They need to share files, share applications, and communicate through e-mail. E-mail and internet are standard for each of these users. Beyond that, it really depends on the user's job responsibilities as to what they have access to. There are various drives located at the corporate location that certain groups might need to access. For instance, each location might have their own folder or drive on the network that only they can see. Then there might be one main human resources folder or drive that all of the human resources groups can access. Then finance might have a drive that is accessible by all users but has subfolders that only their staff can view. So depending on the information, different rights apply for different groups and users. That is how they share information. In addition to that, finance and human resources might need access to the AS400's but the executives and engineers do not. Access to specific applications and systems are only given based on job description and need. There is one other key part associated to this. Some office staff might need to travel or work from home. This is accomplished through a Citrix Secured Gateway[1]. All the user needs is access to the internet from their location and they can connect to the internal network through the firewall. They have access to all the files and applications that they would in the office. If they do not have high speed internet access, an alternate way to get into the network is through a RAS dial-in solution.

Next there is the sales staff. The sales staff is set up very similarly to the office staff. The only difference is that some are GIAC employees and some are distributors working for other companies. The GIAC sales staff is set up exactly like the office staff. The distributors work for other companies and are responsible for their own e-mail, hardware, billing, etc. The only things they need to have access to are current prices, current products, availability, and the GIAC sales staff. This is all available through a secured web server. Prices, products, and availability are all updated by the GIAC staff and the distributors are able to connect to the web site using a unique user ID and password. The user ID and password are provided through the GIAC human resources department. They can do estimates, inquiries, ordering, and communicate to the GIAC sales staff though this site.

Then we have the shop staff. Shop employees consist of shipping and receiving, inventory management, and manufactures. They primarily work on the shop floor and many of them do not need access to any systems. Some of them might need file access and internet access. Others might need AS400 access and e-mail access. System access and hardware access are completely dictated by the user's job description and needs. It is very rare that a shop staff user would need remote access. If it is needed though, it can be provided the same way that the office staff accesses while at home or traveling.

Vendors supply parts and inventory, office supplies, building maintenance, and outside services. They need very limited access to the internal network. Very few of them actually need access to the systems. In some cases, such as a contractor that aids in the maintenance and development of an application, they might need access externally to that application. If they do, they have very limited access and gain that access through a VPN client. If a vendor does require access to the internal network, a unique GIAC user ID is provided through human resources and a GIAC access request form must be submitted and approved.

Customers do not require much access if any at all. Primarily they just connect to our secured web server to review prices, order products, check on status, or just obtain information. GIAC is not responsible for any hardware or applications on their end.

7) Identify four "crown jewels"

A) Customer and contact lists – Since there are so many divisions of GIAC, there are several unique customer and contact lists. First they are broken down by commercial and governmental. Under each of these, different departments are responsible for creating and maintaining the contact and

customer lists. The main departments consist of aircraft sales, parts sales, maintenance, and warranty. All lists are stored on an AS400 system running an application called JD Edwards. This is a secured system and each list can be locked down based authentication of user ID and password. The head of each department decides who has access to which list and what kind of access they have. Some may only have read access and others might have add/change/delete access. Although these lists are not considered to be highly confidential, a reasonable amount of access and authorization is maintained.

B) Contracts – Contracts that are used for purchasing are managed on a corporate basis. All purchasing of goods and services for all locations goes through this one location. This is done in order to reduce costs. By having corporate contracts, better deals are made by purchasing in volume. Plus having all contracts maintained at one location reduces the time spent on them. Having several locations maintain their own contacts is not cost affective. These contracts are stored with three options. One is electronic, second is hard copy, and the third is to have both an electronic and hard copy. Hard copies are stored in a secured vault at the corporate office. A management team is in charge of the vault and checks contracts in and out. There is a master list of who can access certain contracts. The head of the purchasing department decides who has access to what. The electronic versions are stored on a secured network drive. Access to the drive and individual folders are based on user ID and password authentication. The head of purchasing determines who has what rights to which folders/contracts.

C) Management Information – Management information is developed and maintained by the Corporate Human Resources department located at the corporate office. Employees are able to review certain documents at the approval of Human Resources. Documents and information are located in two places. Either on the AS400 system or on a secured network drive. Access to these areas is limited to certain users in Human Resources. Access is secured by user ID and password authentication. Approval for access is decided by the head of Human Resources. One issue that arises is if someone at a distant location needs to review a document. For this, a temporary secured folder is created and limited time access is granted to this information. Based on corporate policy, if a confidential document is printed, it is marked confidential and must be destroyed when it is no longer needed.

D) Bids and Proposals – Out of all the crown jewels, Bids and Proposals is probably the most guarded. The information stored and used involves presentations, quotes, and bids for sales to customers. Some of these involve millions of dollars in sales and if the information got out to competitors, it could be disastrous for the company. The Bid and

Proposals department is located at the corporate office. For physical access to the area, there is a hand scanner that allows access to approved individuals. There are also video cameras located throughout the department. The Bid and Proposal department essentially has its own network. There are 20 employees and each of them has their own computer. It is forbidden for information to be removed from this area. They have their own servers and network equipment located on site. Obviously they still need internet access so they have their own managed firewall. This area has there own network and PC Services specialists that maintain the PC's, servers, and network equipment. This includes intrusion detection, vulnerability scanning, and virus protection. Due to the criticality of this information involved, it was decided to keep them on their own and almost treat them like their own company. This is to reduce the risk of information being stolen or tampered with. The theory is that it is much easier to monitor and maintain a network with a few stations and servers as apposed to mixing them in with hundreds of servers and stations.

8) Insider threat vector each of the crown jewels

a) Customer and contact lists – The customer and contact lists is probably the threat with the least amount of incentive. Some competitors or other parties might be interested in these lists in order to gain operational information. An insider might have monetary incentives. The way that this could be accomplished is by falsifying an access request form. The way our system works is that an online form is available through the intranet. A user would need to have knowledge of the screens and areas of the JD Edwards system that are needed in accomplishing their goal. Once they have this, they simply fill in the information on the form and print it out. After that, certain screens and areas require certain signatures. They are not electronic signatures, they are written signatures. So if the person has the guts, incentive, and access to the required person's signature, it would be possible to forge someone's signature and gain the illegal access. What makes it a little more difficult is that new user ID's and basic accounts are created by Human Resources so it would not be possible to fake an entire user identity. More than likely, the person would need to request the additional illegal access under their user account. When the regular account audits are done, it would be noticed that this person has access they should not have. So it would be possible to gain this access, but it would not be a permanent an unnoticed event.

b) Contract information – Contract information is a more sensitive subject. Government contracts are sensitive due to the nature of dealing with military aircraft. The number of parts, aircraft, etc. being ordered could be some very important information to the right people. In addition, some contracts include specifications of aircrafts being built and sent. From the commercial side of things, it might be important for competitors and stockholders as to who we are

dealing with and what kind of volume is being handled. So overall, there could be monetary or political incentive for an insider to obtain these contracts and sell them or post them on the internet. Since there are two ways to store these contracts, there could be two ways to obtain them. One way is exactly as described as above. What would make this more challenging is the fact that the person would need to know what contracts are stored where and who has authorization to view them. The other way the contracts are stored is in a guarded vault. In order to access contracts in the vault, the vault guard has a master list of who can access what contracts. A non-computer way of obtaining these contracts is to produce a false user badge. User badges are used throughout the corporation to verify identity. They have the user's ID number, name, picture, and magnetic strip. This is what is presented to the vault guard in order to prove identity. Someone could create a false badge with their picture and someone else's user ID and name. However, it is up to the guard to decide if they want to see the person's driver's license in order to aid in the authentication process. So the person might also need to create a fake driver's license which is even more difficult. On top of all that, the person would need to know who has access to which contracts. They would also be taking the chance of the guard knowing the face of the person that is being impersonated.

c) Management information – Management information is not as much of a problem when it comes to business security and continuity. GIAC is a union shop. An employee might have incentive to steal this information in order to get more knowledge of other employee's salaries, position level, etc. Although this would not impact the corporation directly, it could affect the politics, contract negotiations, and ultimately production. There are two systems that this information is available on. One is the AS400 system and the other one is on a network drive. In order to access these systems, a user ID and password is required. Since the user ID's are on the user badges, it would be possible for an internal employee to obtain someone else's user ID. The next thing that needs to be bypassed is the password. GIAC has rules on both systems that lock a user's account with three wrong password attempts. If someone locks their account, they need to contact the Help Desk to have it reset. The Help Desk authenticates the user before resetting the password and unlocking the account. In order to authenticate the user, the Help Desk asks a "key word". This word is something only the user should know. They selected this word upon hiring and it is entered into the user information the Help Desk has access to. As a backup, the Help Desk also has the user's social security number and mother's maiden name. If the user gets the "key word" wrong or forgets it, the Help Desk can authenticate the user by asking both of these questions and get the correct answers from the user. The Help Desk also randomly asks one or both of those questions along with the "key word". So, what follows is a scenario that could occur. Please keep in mind that the person trying to access someone else's account would need to know the person's user ID and be in close proximity to the user. So, the insider trying to obtain someone else's access would need to obtain the user's ID number. Then go to any station and try to login in with the

user ID and incorrect password three times. This would lock the account. Then the insider would have to get in close proximity of the user and wait for them to attempt to login. The login would fail and they would have to call the Help Desk. The insider would then wait to hear the user's authentication word. If they were successful, they would then wait for the right time and call the Help Desk as the user and get the password reset. The intruder is taking the chance of having the Help Desk know that the voice is not correct or the Help Desk might ask them the social security number or mother's maiden name. There is little risk associated with this attempt, but as you can see, it would be difficult and a lot of pieces would need to fall into place.

d) Bids and proposals – Breaking into the bids and proposals network in order to obtain files and documents is the most difficult but poses the highest incentives. Getting this information would be very valuable to competitors or other governments. As stated earlier, the bids and proposals department has their own network that is maintained by their own IT staff. Users that have access to that area must go through detailed background checks and can only get into the area though a hand identification reader. Plus the entire are is monitored by cameras. So in order to steal information, it would be almost impossible unless you worked in the department. What would need to happen is that someone would need access to user accounts, user PC's the network or backup tapes. The only individuals with this type of access would be the higher IT admin staff. There are a limited number of these people so it would be relatively easy to trace back who obtained what information. Plus, any unique changes or maintenance done anywhere in this area is strictly documented. The IT administrators go through a very detailed background check.

9) Outsider threat vector for one crown jewel

For this section, I am selecting the bids and proposals area for the crown jewel. The bids and proposals department goes through very busy times and slower times. When a large proposal is being developed, outside contractors are needed. It is simply not cost effective to keep a full staff on at all times. When there are no bids or proposals being developed, very few resources are required. So at the busy times, outside contractors are a necessity and are hired on. These contractors come from reputable firms and do go through background checks. However, with the amount of money involved with this information, it could be quite valuable to the right person and they might try to bribe a consultant with a good record. So the consultant could be influenced and with the right access, they could destroy, modify, or copy information. Since logs are created whenever someone modifies or deletes information, it would not take long to find the guilty party. However, by that time, too much damage might have been done. On the other end, with all the of new portable mass storage devices available, it is not unrealistic for someone to copy a lot of data, bring it home, and copy it. Surveillance would make this task a little more difficult.

10) Malicious code threat vector for one crown jewel

One thing that could very harmful to the bids and proposals network would be a variant of the "I Love You" worm[2]. This type of worm is spread via e-mail. A PC is infected with this worm, it destroys data, and it grabs all of the contacts that PC has in its address book. Then it spreads the worm to all of the contacts. What makes this tough is that the worm e-mails are coming from addresses of people that they know. So everything looks fine and they open up that attachment in the e-mail. The attachment puts malicious code on the PC and basically destroys data on the infected PC. Then it moves on to the next contact list. This goes on and on until the machines are patched. By this time, a lot of data is lost. This particular worm loves to destroy JPEGs. Bids and proposals are built on pictures and video files. Even though it is not policy, we all know that users save important data on their PC's and laptops but not on the network. If it is not backed up, it is lost. Plus anything that was being worked on at the time of the infestation would be destroyed. This worm could get into the bids and proposals department one of two ways. One is if the worm is so new that it is not seen by the anti-virus or e-mail filtering software and it gets to just one person in the department. It would then spread throughout the department in a matter of minutes. The other way is if an employee has to travel for say two weeks and checks their e-mail remotely. They have not been on the network for a while and have not received the latest patches or virus updates. They receive a worm e-mail and open it without realizing what is going on. They then come back to work and boot up and log onto the network. They are now inside the firewall and the worm spreads.

Even though we are only talking about pictures being destroyed in this situation, it is very possible that other variants of the worm could destroy spreadsheets, word documents, contracts, etc. The possibilities are endless. Even if it is only limited to pictures, it could be disastrous to GIAC. Bids and proposals are the lifeline to the company. Without new customers and sales, the corporation is lost. This department is on a very tight schedule. They need to have the bids and proposals complete, accurate, and on time. If any one of those pieces fails, the sale could be lost. Customers do not care if you are infected or not. They want to deal with competent and reliable people. Days, weeks, or months of work could be lost if a worm such as this hit. That could be the deciding factor of a million dollar contract.

11) Identify the most severe threat

The threat I feel is most severe is a denial of service attack. The greatest risk for this is through a virus or worm. It has been estimated that the corporation loses $100,000 per hour that the computer systems are down. So if one full day of production is lost, we are talking almost $1,000,000 lost. It is imperative that the systems remain up at all times. It has been proven that denial of service for any

period of time can be devastating. Several tools have been put into place in order to reduce the chance of this happening. Things such as firewalls, virus protection, e-mail filtering and intrusion detection all aid in stopping viruses and worms from entering the network. However, there is always a chance of it happening. Although I feel that the network is very stable and reasonably secure, there is a higher chance of a worm or virus getting inside through one means. That is the traveler. Several employees travel with their laptops or bring them home to work after hours. This situation presents a high risk. What can happen is that the user brings the laptop outside the network, plugs into the internet, and gets infected with a virus or a worm. They then come back to work and plug into the network. The virus or worm then spreads throughout the corporation. It is very difficult to keep a laptop up to date on its patches and virus protection. There are systems available to remotely update laptops or not allow laptops onto the network without going out and automatically updating. However, this can be very expensive, time consuming, and hard to manage. One thing that makes it even more difficult is that GIAC has thousands of PC's and hundreds of laptops. Many of these machines are running different versions of certain operating systems. Anything that is hard to manage and maintain poses a very large threat. Something such as laptops that are basically a moving target presents an even higher threat.

12) Recommend a remediation strategy for one of the threat vectors

One of threat vectors I identified was falsifying a system access request form. System access request forms are completed online by the employee or the employee's supervisor. It includes the employee's information and the access that needs to be granted. Then the form is printed out and the hard copy must be signed by the required individuals. Signatures could be from management in the employee's area or individuals outside the employee's area. For example, in order to get remote access through VPN, a Vice President's signature is required. Once all of the signatures are completed, the form is submitted to the Help Desk and the access is granted. Where there is a hole is that signatures can be forged. If an employee wanted to obtain access that they are not authorized to have, they could simply fill out what they want online, print the form, and then forge the appropriate signatures. Granted the employee is taking a big chance of getting caught by the Help Desk or system administrators. A signature might not look right or the unauthorized access could be seen during regular audits of user roles and access. However, it is possible to get away with it for at least a temporary period of time.

I am recommending that access request forms no longer require hand written signatures, but rather, electronic signatures. This can be accomplished through the current Help Desk trouble ticket software called Frontrange HEAT[3]. This software contains all user information such as extension, supervisor, user ID, user name, etc. It is generally used for logging and tracking trouble tickets. However, an access request form page can be created within the software that would be similar to the current online form. The employee's supervisor would

log into HEAT[3] and create a ticket for the employee. By selecting a ticket type of Access Request, a page containing all options of access appears. The supervisor would simply check boxes on the form that go along with the access needed. Based on what boxes are checked, assignments are automatically created for each individual that needs to sign off on the form. When the assignments are created, an e-mail will automatically go to the assignee saying that they have an assignment. The assignee would then log into HEAT[3] and review the access request. If everything looks good, they simply close their assignment. The person that has the assignment is the only one allowed to close the assignment. Once all assignments are closed for the ticket, the ticket is automatically assigned to the Help Desk. The Help Desk now knows that everything is approved and grants the required access to the employee. Once the access is granted, an e-mail is automatically sent to the employee and the supervisor notifying them that the access request is completed. It should be noted that HEAT[3] requires authentication based on a user ID and password. So it is not possible for anyone other than the authorized individual to create a request or to approve and close an assignment. In addition, the employee themselves can no longer create an access request form. With this new process, we have completely locked down and automated the access request system. In addition, all information is now saved electronically for archiving or reporting. No hard copy forms are involved.

It will not be an easy task to implement this new process. Several new accounts need to be created in HEAT[3]. Forms, screens, and rules need to be created in HEAT[3]. Documentation and training needs to be done for employees, supervisors, and IT staff. I will be the project manager for this and I will have several team members. They will consist of staff from the Help Desk, Training Center, and Intranet Development group. The Help Desk administrates the HEAT[3] application and grants access to users based on access request forms. The Intranet Development group administrates and developed the current online access request form. The Help Desk will develop the screens and pages within HEAT[3] based on recommendations from the Intranet Development group. The Help Desk will also create the rules that will handle the automatic assignments, automatic e-mails, and HEAT[3] user accounts. The Training Center will train the supervisors and individuals that sign off on the forms. They will train them on policies and the use of HEAT[3]. They will also send out notifications to the user community concerning the status of the project and key dates. It is estimated that it will take 2 weeks to create the project plan and assemble the team. Then it will take about 2 months to develop the screens, pages, and accounts in HEAT[3]. Then it will take about 1 month to complete training, test, and implementation. So overall it will take three to four months to complete this project.

The only thing that will need to be purchased is additional user licenses for HEAT[3]. The hardware and application are more than adequate to handle the additional load. There will be an additional 120 licenses that will be needed to cover the supervisors and signers that will be logging into the system. Licenses are $150 per seat, so the total cost for this project is $18,000 plus $3000

annually for maintenance.

13) Review the backup strategy

Due to certain policies, it is not possible to backup confidential data to an external removable drive. Therefore it is my recommendation that backups of the local PCs have to be done to a secured department server. The department server will have redundant drives in order to add consistency and availability. In addition, the secured department server will be backed up nightly to the main corporate backup system. This will ultimately allow the PCs to be backed up to the same level as a server. No additional disk space will need to be purchased for the corporate backup system. The corporate backup system backs up data to redundant hard drives and creates tape backups at the same time. Once the data is to the corporate backup system, it is safe. So the question comes up on how we get the data from the PC, to the secured department server, to the corporate backup system.

A software package can be purchased that will transfer data either manually or automatically from the PC to a secured department backup server. That server will then be put onto the corporate backup system roster. Backups of servers on the roster are performed nightly per the normal corporate backup procedure. At that point, we have established secure and reliable backups.

Next is the question of what software and hardware we will use to accomplish this. A server will be purchased and an application called LiveBackup[4] will be loaded on it. The LiveBackup[4] software operates transparently to users, administrators and infrastructure. LiveBackup[4] advertises: "With an automatic, unobtrusive hard drive backup, end-users can work as they always have - without IT training on procedures. Self-serve file recovery brings users back to productivity quickly, without burdening IT"[4]. Backups from the PC to the secured department backup server are done real time as the user is working on their computer. The backups are constant but run in the background with no affect to PC performance. This far surpasses the requirement of backups every 30 days. We are now backing up real time. This software is server and client based. Each PC will have the client loaded. Since there are five members of my department, five client licenses must be purchased. The server application comes free with the purchase of licenses. The cost of each license is $99.00 and the server will cost $8,000. A license for the corporate backup system must be purchased for the secured department backup server. The cost for this license is $1,000. Since these backups will run automatically in the background, no major training will be needed for the owners of the PC's. Administrative training will need to occur for the individuals setting up the server and clients. In addition, training will occur for the PC owners on how to restore their information if needed. A good feature of this software is that the user will be able to restore data relatively easily if needed. Since it is a live backup, recovery data is available instantly. This will save in Help Desk calls and time lost. This aids in the price justification of this project.

For the first year, a total of three hours training per user will be needed. Twelve

hours will be required to setup the secured department server. Four hours of administration training will be needed for each of two administrators for using the software and setting up the clients. It will take one hour per PC to set up the client. This gives us a grand total of forty hours billed at $100 per hour ($4000). For all hardware, software, and time, we have a total of $13,495. After that, a total of $800 per year is required for server maintenance.

14) Review offsite backups

Basically there are two ways to incorporate offsite backup storage. One is to transfer the data over the internet or some type of external network and the other way is to manually transport backup media offsite. Due to the volume of data being backed up, the sensitivity of the data, and budget constraints, I am recommending that manually transporting backup tapes to an offsite location is the best solution. The costs entailed with transferring and storing such a large amount of data over a network with the current technologies just is not cost affective.

With our current corporate backup system, all critical systems and files are backed up at the corporate location. Tivoli[5] Storage Manager Software is running on an RS6000 machine and all backups are saved to tapes that are stored in a tape library machine. Nightly backups are saved to these tapes and the tapes are removed and placed in a container onsite every morning. This system utilizes redundant disk space on the RS6000 for immediate restores. So what happens is that data is in two places (on tape and on hard disks). Each morning there are about a dozen tapes that are stored in a cabinet onsite. The problem with this is that if the building burns down and nobody grabs the tapes, all data is lost. Since all of the procedures and systems for these backups are already in place, it is most cost affective to simply hire an offsite storage facility and ship the tapes offsite daily. This is the best way to do things until technology has improved and/or our budget increases. We will still achieve secure and reliable offsite backups, but with much less work and cost. The only issue with this system is the time it might take to get the tapes back onsite. However, with my recommendation, I would like to find a location that is between one and two hours from the corporate location. This way the tapes are far enough away to miss local damage but close enough for fast response. So overall my approach is to find a dependable and secure facility to pickup and drop off tapes at the corporate location.

After doing some research, we found a company called DocuSafe[6]. This company is located about one hour from the corporate location. They have daily pickups and deliveries. The media is bar-coded for easy retrieval and filing. The way this will work is that DocuSafe[6] will store six weeks worth of backups at one time. Each day between 8 AM and 9 AM, they will arrive and drop off the six week old tapes and pick up the previous nights backup tapes. The six week old tapes are then put back into the tape library. DocuSafe[6] has staffing on site 24 x 7 x 365 and promises to have delivery of media within two hours. This system is faster than if we needed to restore through a network. DocuSafe's[6] facilities are

locked, fitted with alarms, and monitored 24x7x365, safe from unauthorized access. Specific temperature and humidity controls ensure proper conditions in specialized facilities for the short or long term storage of vital information. In addition to double fire doors and a ventilation isolation system, the vault that the media is stored in also has its own carbon dioxide fire suppression system. All security and environmental requirements are met with DocuSafe[6].
Really, the only one time tasks that need to be done are:

1) Adjusting the internal documentation and procedures to reflect the tapes being shipped offsite as opposed to staying onsite.
2) Initial bar-coding of all tapes.
3) An SLA and contract will also need to be signed.

Repeating tasks will consist of:

1) The tapes being picked up and dropped off by DocuSafe[6] on a daily basis.
2) A semi-annual review of the system and DocuSafe[6] facilities will also occur.

For auditing purposes, logs will be kept and maintained as to when and what tapes are picked up and dropped off. Random tests will occur in different weather conditions and times to ensure DocuSafe[6] can maintain the SLA and get the correct tapes to us within two hours.

15) Devise a guerilla business continuity plan

The first step in creating a business continuity plan is to assess the area you want to cover and determine key systems that need to be restored immediately. My office's main responsibilities are testing and documentation. We review and test new technologies, suggest the direction that the business should go in, and create policies and procedures. For our office, the primary need is to get our staff connected back into the network and be able to connect to the corporate network drives. If the situation is going to be long term, test servers and equipment would be required.
My approach is that we hire a disaster recovery company that will be able to supply us with facilities, equipment, telephone connection, and an internet connection. Our office already has VPN access into the corporate systems from outside so that will be the means of connecting in. The company we chose to hire is called Sunguard[7]. Sunguard[7] is a very large disaster recovery company that is able to either supply a building or mobile facility. I am going to base my recommendation on a mobile facility. The closest Sunguard[7] location is about three hours away so it would be difficult to establish our office there. A mobile facility is basically a fancy semi equipped with necessary equipment and desks. They are able to be at any location we specify within a 24 hour period. The equipment we will require them to bring on the semi is three telephones, two printers, five complete PCs, and two standard servers. We have a parts center located about 45 minutes from our location. That is the location that we will

establish phone and internet service. That is the location we will have the semi set up. It is far enough away to be away from any local disaster but close enough for everyone to travel to. We will also setup a disaster box that we will put vendor names and numbers, internal contact information, disaster recovery plans, licensing information, and copies of necessary software. This disaster box will be stored at our offsite tape facility. The will be able to drop this box off at our temporary location. The equipment that will be on the semi will not have anything installed. So once the semi and disaster box arrives, we will be able to start the recovery. We will load operating systems and necessary applications. This process will take less than 12 hours. So it is estimated that if our office is destroyed, we will be up and functional within a 36 hour period. We can then remain this way indefinitely. As long as we save all new data being created to the network drives, we will be able to transition back to a permanent location very easily. Now that we are creating nightly backups of each of our PCs, all we need to do is have the offsite tape storage company drop the backup tapes off at the corporate location or wherever the corporate backup system is located at the time.

The one time tasks will be creating the initial inventory list for Sunguard[7] to use, the initial procedures, disaster box, and add the disaster box to the offsite storage facility inventory. Repeating tasks will include adding or removing equipment to the inventory list, updating the disaster box as needed, updating the procedures as needed, and practice runs yearly. We audit the procedure once every year by doing an actual run through of the entire process. We will review and update the disaster box contents, inventory list, and procedures once every three months or as changes occur.

This recommendation would be very easy to implement throughout all of IT operations. In fact, that would fall under my office's responsibility. Since our office is responsible for corporate wide integration and procedures, this would be a perfect opportunity consolidate services and save money. All we would need to do is get a list of critical business systems from each division and a plan on recovery. Then we would just add these items to the inventory list or create separate inventory lists for Sunguard[7]. Then we would create separate disaster boxes for each area to be stored at our offsite storage facility. We would probably need to hire additional resources to keep things up to date, but our plan would definitely be able to integrate the entire IT operations areas. The additional thing I would like to put in the plan if we would do this, would be to create two network stations that could connect directly into our internal network. That way, speeds would be increased, things would work more seamlessly, and we would not have to depend on the internet.

Although we are a manufacturing corporation, we could still use my basic approach in order to provide business continuity throughout the corporation. It would simply include an offsite location to store critical hard copies of documentation and some equipment. Next we would have alternative locations for different offices and facilities. This might be other corporate locations or temporary locations. It would just be a matter of making sure all required equipment is available within a timely manner.

16) References

1. Citrix Systems Incorporated. “Citrix Secured Gateway 1.1.” 5/27/2002 http://infosysinc.com/MRC/content/IT%20Security/Citrix/Citrix_Secure_Gateway_Datasheet.pdf (8/31/2004)

2. Lemos, Robert. “Inside the I Love You Worm”. 5/4/2000 http://zdnet.com.com/2100-11-520463.html?legacy=zdnn (8/16/2004)

3. Frontrange Solutions. HEAT Product Home Page. http://www.frontrange.com/heat/ (8/23/2004)

4. Storeactive. LiveBackup Product Description Page. http://www.storactive.com/solutions/liveBackup/ (8/16/2004)

5. IBM. Tivoli Storage Manager Product Description Page. http://www-306.ibm.com/software/tivoli/products/storage-mgr/ (8/19/2004)

6. DocuSafe Records Management. DocuSafe Services Home Page. http://www.docusafe.com/media.html (8/19/2004)

7. Sunguard. Sunguard Services Home Page. http://www.availability.sungard.com/ (8/19/2004)

Last Updated: October 24th, 2017

Upcoming Training

Community SANS Portland SEC301	Portland, OR	Oct 30, 2017 - Nov 03, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Ottawa SEC301	Ottawa, ON	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
Community SANS Austin SEC301	Austin, TX	Jan 22, 2018 - Jan 26, 2018	Community SANS
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
Southern California- Anaheim 2018 - SEC301: Intro to Information Security	Anaheim, CA	Feb 12, 2018 - Feb 16, 2018	vLive
SANS Brussels February 2018	Brussels, Belgium	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS New York City Winter 2018	New York, NY	Feb 26, 2018 - Mar 03, 2018	Live Event
Community SANS Chantilly SEC301	Chantilly, VA	Mar 05, 2018 - Mar 09, 2018	Community SANS
SANS Secure Singapore 2018	Singapore, Singapore	Mar 12, 2018 - Mar 24, 2018	Live Event
SANS Northern VA Spring - Tysons 2018	McLean, VA	Mar 17, 2018 - Mar 24, 2018	Live Event
SANS Secure Canberra 2018	Canberra, Australia	Mar 19, 2018 - Mar 24, 2018	Live Event
SANS 2018	Orlando, FL	Apr 03, 2018 - Apr 10, 2018	Live Event
SANS 2018 - SEC301: Intro to Information Security	Orlando, FL	Apr 03, 2018 - Apr 07, 2018	vLive
SANS Security West 2018	San Diego, CA	May 11, 2018 - May 18, 2018	Live Event
SANS Northern VA Reston Spring 2018	Reston, VA	May 20, 2018 - May 25, 2018	Live Event
SANS Rocky Mountain 2018	Denver, CO	Jun 04, 2018 - Jun 09, 2018	Live Event
SANS OnDemand	Online	Anytime	Self Paced
SANS SelfStudy	Books & MP3s Only	Anytime	Self Paced