Global Information Assurance Certification Paper

Information Security Fundamentals+

GISF+ Practical Assignment
Version 1.0

Vicki Gillis
December 28, 2003

Summary

Fresh out of the SANS Information Security Fundamentals course, this paper is about my first few weeks at GIAC Enterprises. It gives examples of security challenges at GIAC along with cultural behaviors towards security.

GIAC has a number of assets that have specific security needs including a patch management program to protect the network from vulnerabilities such as viruses. And although GIAC has a comprehensive back-up strategy, this paper explores how small groups can protect themselves by making extra backups of important data without a big expense.

Starting From Scratch at GIAC

"What did I get myself into?" This is a thought that crossed my mind several times after I accepted the job with GIAC Enterprises. Fresh out of security training, I applied at GIAC Enterprises, I had just completed my Information Security Fundamentals certification and I was eager to get started in the security field. The job posting that appeared on Monster.ca stated that the position was for a Security Analyst at a large corporation. I quickly applied, jumped through all the interview hoops and landed myself the job! I proceeded to pray that my SANS course and certification were enough launch me into my new career as a security professional.

The first few weeks at GIAC were an eye-opener. I went from thinking that I knew something about information security to learning that I had a lot to learn about information security. I don't want to get a head of myself so I'll start out by describing the first few weeks and my first few assignments.

The Run Down on GIAC Enterprises

GIAC Enterprises is a large transportation company; they specialize in shipping merchandise all over Canada and the US. This large organization has approximately 19,000 employees and approximate annual revenue of $6 billion dollars. The majority of the revenue is generated from transportation, however a

small portion is also generated by what is called “charged service”; this is revenue generated from when GIAC stores or inventories merchandise for a customer, or another example is when GIAC charges a customer for the extended use of equipment.

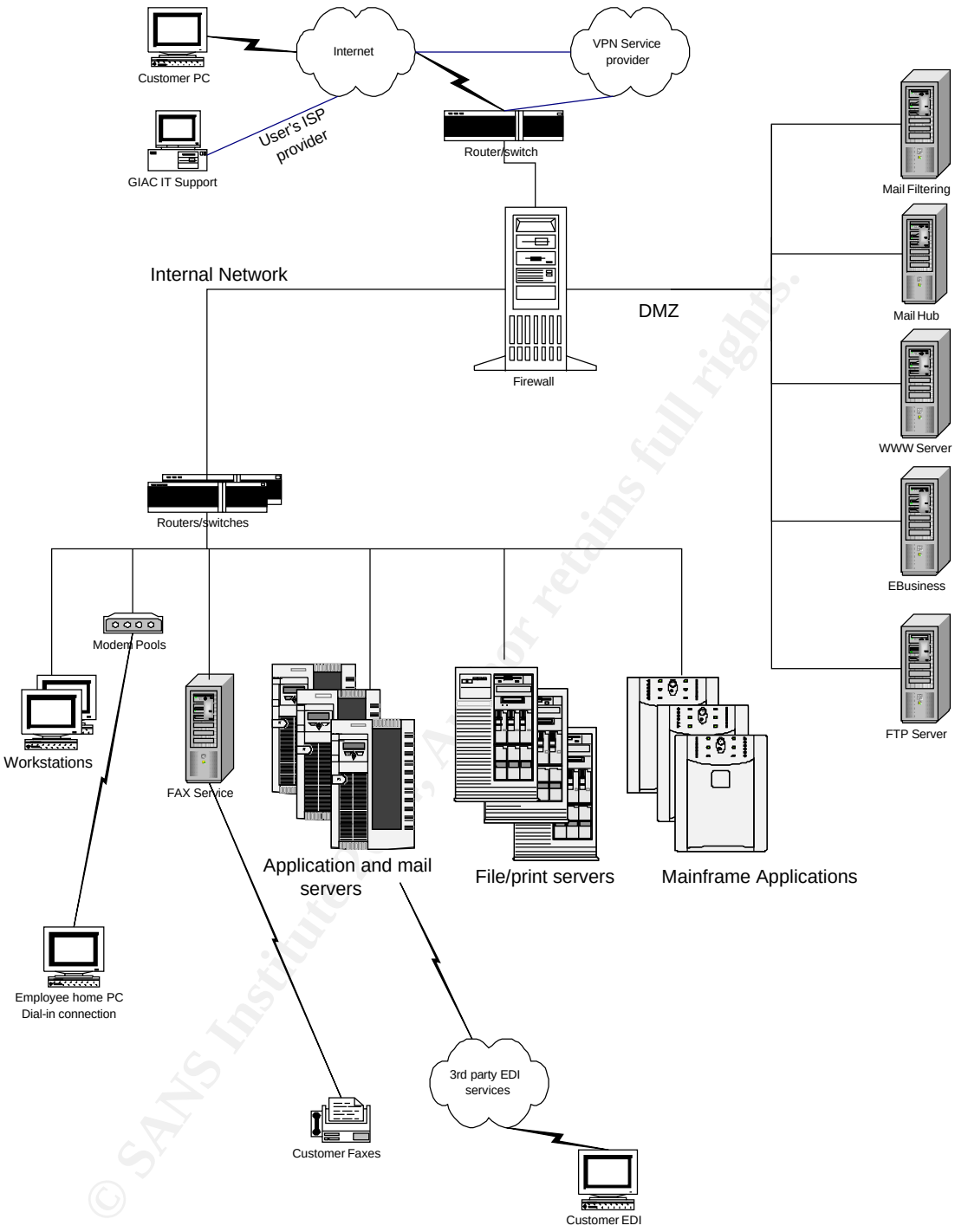
Out of 19,000 employees the vast majorities, 16,000, are unionized forces whose salaries are negotiated through collective agreements, their salaries range from 45,000 to 65,000 plus benefits. Approximately 3000 employees are management employees, these employees are divided into three categories: middle ($40,000-65,000), senior ($50,000-90,000), director ($100,000+).

The Information Technology department has only one main location, it is in the main headquarters building and having over 350 employees it occupies several floors. IT is an integral part of GIAC, they contribute to the total revenue by supporting, maintaining and optimizing they use of information systems. The overall IT budget is $68 million for operating expenses and $120 million for capital projects.

IT is split into two distinct groups: operations and development. The operations group is further split into network operations and data center management, system administration, security and help desk. There are approximately 300 servers that are supporting approximately 100 applications, network, file and print services, and common services such as email and fax.

IT Infrastructure

The following diagram is a high level diagram of the network. The GIAC network diagram shows that there is a two-legged firewall: one leg is the DMZ and the other is the private network. GIAC has only one production zone with all applications and file and print servers connected. Users can either be directly connected to the network if they are on the premises or they connect directly via a dial-up connection. There are exceptions for IT support people: GIAC has a VPN service provider and users are authenticated by user id, password and token id.



The Security Group

The security organization recently underwent a transformation. In the past, the security group's main focus was access control (add, change, delete access) for GIAC computer resources, now there are two security groups: one group who

manages access control and the other is governance and guidance. The governance and guidance group is lead by the new CISO, who is my boss. She reports to the director of IT operations, and he reports to the CIO.

Our security group is called Corporate Information Security, and the CIO formalized it approximately six months ago. Up until then GIAC's security practices were informal and lacking in consistency and that, coupled with the CIO being concerned by all the warnings of viruses and vulnerabilities on operating systems forced him to formally appoint a CISO. Since then, my boss has been putting together a team and she has been defining the corporate security program.

As a group our mission is to provide governance and support in the area of security for information technology so that IT can guarantee the availability, confidentiality and integrity that GIAC Enterprise requires to continue doing successful business with its customers and partners.

The security group is broken up into four areas:

Area	**Staff assignment**
Network Security	2 full time employees
Compliance and Monitoring	1 full time employee
Architecture and System Certification	1 full time employee*
Disaster Recovery	1 full time employee

**under evaluation*

Two employees are assigned to network security and their primary focus is working with the system administrators and network analysts to develop standards and procedures for secure network operations.

The compliance and monitoring area is slowly developing, one person now occupies this function as an analyst, his main objective is to define requirements and set up monitoring on critical applications. His work in this area has been minimal to date as GIAC has recently been struggling with applying anti-virus updates and security patches on computers and all of his focus has been in this area.

Architecture and system certification: this is my area, which I will describe in more detail further on.

Lastly, there is the position of disaster recovery, this person works closely with the network operations group to ensure that the backup and restore procedures are keep up to date, and he also participates in the planning and execution of a regular disaster recovery exercise.

The CISO's budget is approximately 4.8 million dollars; $800,000 is operating expenses that cover things like salary and benefits. The balance is allotted for security services or products such as monitoring tools. The total is approximately 3% of the IT budget. Although the money is in the budget, all IT projects must demonstrate that the spending will support GIAC's core business functionality. Projects are reviewed by a committee made up of business, financial and IT senior managers and directors.

My first few days at GIAC I familiarized myself with the office. Each employee at headquarters has there own "cube", the senior managers and directors at GIAC are assigned closed offices. Cubes and offices are equipped with a telephone and a PC or a laptop, a filing cabinet and some basic stationary supplies. The PCs and laptops differ in makes and models but they are loaded with standard images of Windows XP. .

Employees working in the headquarters building are issued photo ids cards that must be carried when entering the building. I later learned that some of the other bigger locations also have id cards, but some employees working out in the field may not have cards. Certain floors and certain rooms, such as the data center, have additional card readers that are active 24 hours a day, and to gain entry an employee must swipe his or her card.

Each member of the security group has a laptop. Employees who travel are usually given priority and although my only travel may be for training, having a laptop would give me more flexibility for working remotely. My supervisor provided me with my accounts and passwords to Email, the network, Internet and remote dial-in access. These, I was told, are the basics. Almost all employees with access to a computer get these standard accesses.

Security Architect

Getting started as a Security Architect was not easy since it was a brand new position and there was no framework to support the function. My main responsibility is to interact with the development side of IT and ensure that all new applications developed (or enhanced) are following good security practices. Once a system has completed development then they must be certified for production, this means they have to demonstrate that all recommendations that were previously made have been addressed. It sounded good, lets hope that it's worth the whooping $55,000 a year I'm being paid!

As a Security Architect I needed to develop a methodology for following up on new applications in development and tracking their progress to production. My success, end the end, would be measured by:

- My ability to evaluate projects and identify risks

- My ability to provide feedback regarding security controls which could mitigate the risks
- Documenting a presenting risk assessments in meaningful way so that business units could make informed decisions about security
- The creation of checklists and test plans to support the developers

Since GIAC has many applications, once a methodology is in place my boss will evaluate the need to hire additional help in this area.

My secondary responsibilities are shared with a colleague; it is our responsibility to maintain the information security policies and procedures. Our success is measured by:

- How often the security policies need to be reviewed (the less often the better!)
- Quality of procedures – ensure they are useful for those who require them
- Policies cover all information security areas at GIAC
- Information is disseminated to all those affected

To develop my methodology as a Security Architect I needed to understand the different types of projects that would go through development so the CISO recommended that I do analysis of the different business processes. My mission was attempting to understand at a high level the different processes and cycles that our company has and document my findings. After that she asked that I take a few key areas and examine where there could be room for improvement.

GIAC: The Business

The major business processes can be broken out into five major categories:

- Sales
- Deliver
- Collect
- Plan
- Support

GIAC's primary business is transportation, shipping merchandise all over Canada and major locations in the United States. The customers are very diverse and their commodities vary, for example: lumber, automotive, farm produce, etc.

GIAC is broken up into six business units to support the five major processes.

The sales organization does just that – it sells. They talk to the customers and bring in the business. They handle all types of customer information such as:

- contacts
- addresses
- contract information and pricing information

- opportunity information

The delivery or transportation organization has the job of making sure we can deliver what we promised. They manage information such as:

- trip plans
- asset utilization information
- shipping traffic
- safety

Our collection or finance department is then responsible for billing the customer and collecting revenues. They require access to the information outlined above to accurately bill the customer and collect.

Planning is a strategic group at GIAC and they focus their work in three areas:

- Business planning and corporate strategies
- Financial planning
- Asset planning and service planning

And lastly the Support organization provides value in the areas of inventory, asset maintenance, human resources and supply management.

The information technology department supports all the systems that are used in the business processes. The diagram below shows the systems in black and the users in blue.

<table>
<tr><td rowspan="2">Business Applications</td><td colspan="4">All Users

Email
Intranet/Internet</td></tr>
<tr><td>Sales

E-Business
www
Marketing Apps
Customer databases</td><td>Delivery

Transportation

Crew Information/Time Reporting</td><td>Collections

Revenue management
Pricing</td><td>Planning and Support

Enterprise resource systems
Purchasing</td></tr>
<tr><td>Infrastructure Support</td><td colspan="4">Information Technology

Architecture & Development
Computer Operations & Support Services</td></tr>
</table>

Obviously our customers are an integral part of making GIAC the company it is today. Customer information is first introduced into our systems by the sales

group. Once a customer is in the database we can then start to receive shipment requests from them, and they may be in the form of electronic data interchange (EDI), requests submitted over our Internet or fax.

EDI is always set up with the help of a value added network. EDI is not sent directly from the customer to GIAC, it passes through a 3rd party who manages the data flow.

If a user would like to submit a shipment request directly, they are issued a user id and password to access our Internet site. There, they can make requests and query their information for other shipments.

Lastly, customers can fax in their request to a central processing facility. All faxed requests are manually enter into GIAC system by a customer service representative.

The Assets

After having compiled some information on the various business processes, I was now in a position to identify some important information assets. For the purpose of this tale and my own sanity, I limited myself to four distinct areas: customer information, personnel information, contracted services information, and the transportation application that control the operations of GIAC. The following is a brief description of each asset and how it is used, stored and maintained.

Customer Information

Customer Information flows into the company via the account representatives in the sales group. It is used by all different business units in the organization. Some information is static, such as, contact information and billing information; other information is not so static such as location and destination of shipments and merchandise information. All these pieces of information could be obtained in several different systems. This, of course, was normal due to the whole business process: it was available to our account representatives through our marketing and Customer application, it was available to the transportation organization through the operational applications so that shipments could be picked up and delivered, and it was available in our revenue systems so that finance could bill and collect.

Customer information seems to be widely spread across the organization and may be vulnerable to misuse by individuals who seek to gain financially or in other ways.

Contracts and Consultants

Since GIAC is such a large organization I decided to focus my research in the area of IT processes with regard to contractual services, I discover that it is overwhelming; so many systems, so many different configuration processes so many different requirements. However, I did find one small common element that I decided to focus on: development projects mostly use outside consultants when choosing new applications, software, hardware, etc. Consultants ranged from independents to large vendors and their involvement ranged from design to implementation.

This caught my attention simply because there seemed to be so many outsiders that had critical information about GIAC applications and our IT infrastructure. I also learned that there was no clear practice for hiring consultants and no one person or group could accurately say how many consultants were at GIAC at any one time. I found out later that this was not only true of IT but also throughout the organization.

In addition to this, IT also has a high number of service level agreements (SLAs) with vendors to support the IT infrastructure. Information about SLAs is generally kept on the network file servers which, for the most part, are generally accessible by the IT department. Negotiations of SLAs generally are passed between various IT groups via email and then final versions are stored on the network for reference.

It was easy to draw a conclusion that anyone working on the premises of GIAC (employee or contractual) could obtain information about vendor services and pricing agreements. Trust seemed to be the only control mechanism, and it was an area where the risk of disclosure of information could potentially be harmful.

Employees

Next, I decided to understand some of the back office practices and I decided to focus in on the employee information. Since I had just been hired I thought that this could be an interesting area of research I had no idea what was in store for me.

I started by talking to the human resource liaison in IT. He explained that each department at GIAC followed basically the same hiring practice but also each had the liberty of managing information in there own way. Once an employee is hired, basic data is entered into the enterprise resource application. This application is the central repository for all employee related information: salary, time and schedules, organizational data, qualifications and performance. It also interfaces with several smaller applications that serve as mechanisms to collect HR information. For example: performance evaluations are done in a form based application created specially for reviews. The evaluation and comments remain in the smaller database but the overall results are fed into the enterprise resource application so that an employee's compensation can be adjusted.

Other HR related practices differ from one department to the next, for example: all employees are required to enter time information in the payroll system, but some departments choose to centralize this function by having a clerk input all the information while other departments choose to have individual employees enter their own time. Managers and team leads are responsible for accurate time recording.

I discovered that this type of flexibility applied to all employee related practices: although all employee information resided in one complete enterprise resource system, how the information got there, who put there and who had access depended the department.

I felt that some of the issues we could be facing here involved protecting employee information; I knew that there were laws pertaining to this so I decided to mark this as a high priority. Although I knew if would be difficult to address all the departments and their processes I jotted down some ideas about having clerks and HR representatives sign confidentiality forms and provide them with some documentation of the privacy laws that govern the information that they manage.

Transportation application

For GIAC to effectively manage the transportation of merchandise for its customers in a timely manner and fulfill customer expectations, it is important to be able to access the transportation operational application. This application contains information about pick-up and delivery locations, preferred routes, schedules, merchandise release information, required equipment to move merchandise, etc.

This information is not only absolutely critical to the operations people who coordinate the shipments, but also the customer support representatives, account managers, billing clerks and transporters. Shipment information comes into GIAC via fax, electronic data interchanges and the Internet.

The Disgruntled Employee (a.k.a the insider)

It seemed to me that identifying important assets and defining how to protect them could prove simple enough, however I did not know how I could justify my reasoning. I could see that GIAC did not have strong security notions. I needed to demonstrate where the risk was and allow the company to make the decisions.

My first area of focus would be the inside threats that could affect GIAC. I needed to decide on something that would really hit home so that my boss could sell the concepts to her superiors. Thinking back I remembered an article that

some of the biggest threats to a company were its own employees: harm could be done intentionally or unintentionally.(Bruck 2002)[1] Slowly I narrowed my focus to the "disgruntled employee". In a company the size of GIAC, surely there have been a few disgruntled employees, and I'm sure that in the IT department there have been a few over the years.

For each of the four information assets that I described earlier, I created a matrix to show the threat (i.e. the disgruntled employee), the vulnerability and the risk.

Asset	Motivation	Vulnerability	Risk	Control
Customer Information	Employee could sell the list /financial gain	Information is available from a number of different sources	Disclosure	Training and awareness
Contract Information	Financial gain	Weak storage practices	Loss of trust	Strong access control procedures Training and awareness
Management Information	Curiosity	Weak change management process – possibility to introduce custom code	Disclosure	Code review Segregation of duties Change control procedures
Transportation System Information	Cause a slowdown Cause disruption in business	Easy access to pre-coded exploits *Bruck 2003[2]	System becomes slow or unavailable	Patch Mgt process Change control process

[1] Bruck 2002
[2] Bruck 2003

The Outside Threat

My understanding of threats is continuing to grow however; I wanted to show the CISO that we should not only focus on our internal threats but also on our external threats such as virus attacks, hoaxes, denial of service or social engineering.

Hoaxes can be just as damaging as a virus to a company such as GIAC. Early in the year users were targeted by an email hoax, the content stated that Microsoft was sending out patch information.(Gaudin 2003[3]) This caused wide spread panic and certainly disrupted operations for hours. It also unnecessarily clogged the Help Desk and this in turn blocked legitimate user problems from being solved quickly.

MS Blaster strikes GIAC

GIAC Enterprises is also struggling with anti-virus and patch management as I have previously mentioned. Although there have been incidents of virus infections, such as MS blaster, GIAC has only felt small interruptions.

MS Blaster infected 90 or so employees and a couple of print and file servers. It stopped short of infecting some application servers because of the aggressive measures taken to install patches on all critical systems. Users reported problems to the help desk when they started noticing slowdowns on their computers or their PCs rebooted on their own.[4] The Blaster is explained by Symantec as a "worm also attempts to perform a Denial of Service (DoS) on the Microsoft Windows Update Web server (windowsupdate.com). This is an attempt to prevent you from applying a patch on your computer against the DCOM RPC vulnerability".[5]

The network operations people started rapidly applying security patches to all Windows platforms, starting with the critical systems then moving to the less critical ones.

GIAC was lucky in that it only slowed down our people inside, it did not affect the transportation operation or customer service. GIAC has several applications running on Windows 2000 servers, applications that allow the financial department to support the "bill and collect" portion of the customer cycle process. Although this part of the business could survive for a few days without the applications we would be limping along and it is clear that this would affect our

[3] Gaudin 2003
[4] Microsoft 2003
[5] Symantec 2003

core business over time but GIAC could tolerate down time as long as a solution was in sight.

Patching systems and keeping our anti-virus up to date has been a growing concern since August. One of team members has been dedicated to this initiative and is responsible for defining the process and monitoring the execution.

The Severe Threat

The most severe threat that could affect GIAC is an attack on our network that renders transportation systems unavailable for more than six hours. After the six-hour threshold our customer commitments begin to deteriorate. Contractual agreements are not upheld. We also can start to inflict damage on our customers by not having their merchandise at its destination in time. For example: a manufacturing plant waiting for a scheduled shipment of widgets to manufacture their product may have to stop production lines if we do not honor the shipment agreements. Financial loss starts to accumulate after six hours and can quickly rise into hundreds of thousands of dollars. Transborder shipments are the most likely to suffer if we are not able to produce required government documents at the time of crossing. Of course, the documents can be produced manually but generally this could take hours.

In light of recent events with common platform vulnerabilities, GIAC feels that the likely of a threat is "low" but the impact is "high". This means GIAC had to give it some serious thought and put together an action plan.

Remediation for the Severe Threat

The remediation strategy for protecting GIAC's network is a proactive patch management program. There are many groups that need to be involved in such a program at GIAC, they are:

- Security: for identification, coordination and analytical skills
- Network Operations, System Administration: for technical skills
- Help Desk: for communications

Following is a brief overview of the program steps:

- Identify vulnerability: this could be done using security services such as Symantec[6]
- Assess the risk of the vulnerability
- Notify network operations people and system administrators

[6] Symantec 2003

- Test patch
- Deploy patch
- Notify, if applicable, third parties that may be affected or who may subsequently affect us
- Notify end users and remote users
- Monitor and check for compliance

In the case of anti-virus signatures needing updates then additional steps may need to be taken such as:

- Deploy anti-virus signature using automatic agent
- Monitor and check for compliance

The tools required for this type of process to work are:

- Alert service providers
- Automatic agent for deploying anti-virus
- Lots of man-power or automatic agents for deploying patches on network servers
- Email for notifications
- Internet access for those users who need to download the patches for themselves (i.e. remote or 3rd party)
- Help desk services for reporting problems encountered

The time it takes to keep this type of program working depends on the threat. The greater the threat (i.e. new virus) then the shorter the implementation time should be, however, regular releases may be scheduled. The following table is an example of implementation times:

Task	Low risk	Medium risk	High risk
Identify & Assess risk	9-15 hours	6-9 hours	3-5 hours
Notify groups	3 hours	2 hours	1 hour
Test patch	36-54 hours	24-30 hours	12-18 hours
Deploy patch	108-144 hours	72-80 hours	36-48 hours
Notify: - 3rd parties - end users - remote users	12-16	6-8 hours	3-4 hours
Monitor and check for compliance	On-going	On-going	On-going
Total time	240 hours	120 hours	72 hours

The key for this type of process to work is good communication and effective identification of vulnerabilities that can negatively impact GIAC.

Our own back-ups

After submitting the plan for stronger patch management my boss felt quite comfortable in assigning me some additional duties.

She explained to me that since our group been documenting policies, procedures and processes that we needed to ensure that our files were protected in the event that our computers crash or a file server is corrupted. She asked me to put together a few high level recommendations to ensure that our group follows secure back-up procedures and I should also draft a plan for implementation.

I proceeded to interview my colleagues, all, without exception, have been keeping information on local drives to protect it from prying eyes and to protect it from being altered or deleted. The first thing I decided to do was to pull out the dusty version of our policy on company document storage and handling and circulate it among the group. This policy is important because it explains how all documentation is the property of GIAC and precautions should be taken for handling and storage.

I proceeded to then draft out the steps we should take to protect our files:

- Create a file on the network with an access control list limited to our group.
- Encourage group members to store a copy of all files in this directory. This would mean that they would be backed up under the corporate back-up process. No additional hardware or software would be required because the existing Windows 2000 infrastructure would be used.
- Encourage group members to use the directory in their local system, such as My Documents, so that regular individual back-ups could be taken.
- Distribute and train colleagues on the use of personal storage devices such as USB devices. Generally the USB storage devices are equipped to make transferring files very simple.
- Once a week, prior to staff meetings, employees will be asked to synchronize all files in their My Documents to the external storage device.

The steps outlined above are simple and easy to audit. Most of the tasks are one-time tasks and do not have large dollar amounts tied to them. USB storage devices can range 50.00$ to 200.00$ for reasonable storage space, and they can be reused for each backup. As for time, this type of solution only costs the employees a few minutes a week.

Employees will be reminded during the staff meeting that they should have backed up their data and the USB devices should be kept off site and not left at the office.

Simple plans such as these are perhaps not suitable for a large corporation, such as GIAC, to deploy so the network backups must be 100% reliable and users must be made aware of existing policies. Regular disaster recovery exercises can generally flush out any technical problems, and regular security awareness programs remind users of the importance of careful storage of information.

Off Site Backups

A backup strategy for GIAC can be very complex, however since the company has many sites it would make sense to leverage one of those sites to act as a backup recovery site. Providing that the right infrastructure could be put in place, such as communications, hardware and software, GIAC could manage to do the following:

- Choose appropriate off-site location using "not too close or not far" criteria, for example, not too close in the event that there is a downtown disaster that it would be unusable, and not too far so that key personnel can reach it quickly.
- Prepare a room in an off-site facility: tape storage devices, PCs, office equipment, tables and chairs, stationary, etc. Using a room that is part of a GIAC facility ensures that it is always available and it removes the cost associated to third party vendors who offer this type of service.
- Determine how often data needs to be backed up. This could be as little as every ten minutes or as long as one day.
- Write data to tape storage devices that are located at a remote location.
- Ensure rooms that are receiving this data are just as secure as the central computer rooms by using access cards, cameras, fire and flood control, etc. This type of security is important to ensure the integrity of the tapes, only authorized people should be allowed in the off-site backup room so that tapes are handled according to a pre-set policy.

In a scenario such as this, GIAC would require around the clock monitoring of the room, this could be done from the central command center in the headquarters building. Also, full time monitoring that the backups to ensure that they being correctly written to tape and the storage devices are not malfunctioning. It would also be important to ensure that all new applications being developed be part of this global backup strategy, this means that the tasks of determining what backups should be taken and monitoring are always on going.

The key to ensuring that this type of set-up would work is to test it regularly in disaster recovery scenarios.

Keeping our security office going

Now that the security team is keeping secure backups, it was time to look at how we would keep our office running in the event that our facility became unavailable. It was difficult to know where to start so I met with the team to discuss what our requirements would be.

As previously mentioned, the security team has four areas of focus: network security, compliance and monitoring, architecture and disaster recovery. And in each of these areas our documentation on policies and procedures are our most important asset. Take for example disaster recovery; our team is responsible for ensuring that all other areas in IT kept the disaster recovery plan up to date. But what would happen if the plan were lost, would we know what to do?

This is the high level strategy I proposed that we take to ensure that the security team could continue business. Every three months the IT teams must review their procedures for disaster recovery, procedures are updated and sent to the security team. The main disaster recovery manual is updated and re-circulated. This is where the current process ends, so this is where my plan begins.

After each team reviews their section of the disaster recovery plan and the main manual is updated, a copy should be stored on an external storage device such as a CD, DVD or USB device and hard copies should be printed. Once this has been done they should be put in a sealed envelope and sent to off-site to a near-by facility, all parties who have steps in the disaster recovery plan should be made aware of the location of the plan and they should be instructed to print copies for themselves.

Although this is a small step in keeping our office afloat, it ensures that one critical piece of information is available in the event of a disaster. Starting with one small piece can help us move to slowly in the right direction. Other offices can take similar approaches by ensuring they know where to go for information in the event of a disaster.

We can audit this approach by retrieving the document at the backup site and ensuring that it is not more than three months old, and we can upload the information on the external media device to ensure that it can be retrieved.

Identifying critical procedures, ensuring that procedures are up to date, documented and retrievable will ensure that employees have an easier time of recovering from a disaster. Rehearsing or auditing the retrieval of procedures and application of procedures can also ensure that employees know their role in a disaster recovery and it will ensure that the business can keep on going. It can easy by applied all over the company: identify, document and practice. The key to this is ensuring that you look at only what is important to keep the business running. If each department looks at only the essentials GIAC has a better

chance and being able to recover from a disaster. Of course it is wishful thinking that a corporation of this size can exercise plan every three months, but there should be at least a yearly exercise with all departments involved.

Large organizations move very slowly and even more slowly in the direction of information security. The appointment of security teams is generally a good step in the right direction. Risk assessment methodologies exist widely over the Internet, and there are thousands of information resources available to help the security cause. Starting slowly and talking to the business representatives brings about a gradual change in culture and this seems to be starting to work at GIAC.

Here is to hoping that not every day will be faced new security vulnerabilities and we will learn to pro-act rather than react.

References

Bruck, Michael. **Security Threats From Within**. URL: http://www.entrepreneur.com/Your_Business/YB_SegArticle/0,4621,298386,00.html . April 2002

Bruck, Michael. **Dealing With Internal Security Threats**. URL: http://www.entrepreneur.com/article/0,4621,308373,00.html . May 2003

Gaudin, Sharon. **Warning Goes Out About Blaster Email Hoax**. URL: http://itmanagement.earthweb.com/secu/article.php/3065081 . August 2003

Microssoft Corporation 2003. **What You Should Know About the Blaster Worm and Its Variants.** URL: http://www.microsoft.com/security/incident/blast.asp . August 2003

Knowles, Douglas. Perriot, Frederic. Szor, Peter. **W32.Blaster.Worm**. URL: http://securityresponse.symantec.com/avcenter/venc/data/w32.blaster.worm.html . August 2003

Symantec 2003. **Deepsight Alert Services**. URL: http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=160&EID=0 .

Last Updated: October 18th, 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
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 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