GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Introduction to Cyber Security (Security 301)"
at http://www.giac.org/registration/gisf

GIAC / GISF +

Information Security Fundamentals

GISF – Basic Practical Assignment Version 1.0

July 2003

Taylor Trimby

Track 9 - Information Security Fundamentals + (GISF)
All students beginning certification after to July 25th, 2003

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table of Contents

Section	GIAC Health Processes	Page
	Abstract of Paper	3
1	Description of GIAC Enterprises	4
2	Diagram and Description of GIAC Enterprises	5
3	Describe your office or department at GIAC Enterprises	6
4	Describe your Job Description at GIAC Enterprises	7
5	How does GIAC conduct its business?	8
6	What applications and/or what type of access are required to carry out these business operations?	9 -10
7	Identify three "crown jewels" your office has access to and is responsible for	11 - 12
8	Insider threat vector for each of your office's crown jewels	13 - 14
9	Outsider threat vector for one of your office's crown jewels	15
10	Malicious code threat vector for one of your office's crown jewels	16
11	Identify the most severe threat	17
12	Recommend a remediation strategy for one of the threat vectors you have described	18
13	Review the backup strategy	19
14	Review offsite backups	20 - 21
15	Devise a guerilla business continuity plan	22
	References	23
	GIAC Health Network Diagram	24

Abstract / Summary

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

This document will focus on the GIAC Health Corporation, a small Midwestern Hospital organization that is compromised of 3 hospitals, 2 long term care facilities, corporate office and data center.

The Information Technology department will be spotlighted and GIAC Health's crown jewels, access and possible threats to those jewels will be further identified.

Finally, this document will review backup possibilities, and a business continuity plan.

© SANS Institute 2004, Author retains full rights

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.) Description of GIAC Enterprises

GIAC Health (Enterprises)

GIAC Health is a small non profit Hospital Organization that has been providing primary health care to the surrounding suburban area for over 100 years. The corporation consists of 3 hospitals that average 300 beds each, 2 long term care facilities, one corporate office and one data center. The corporate office and data center are located on the same campus. GIAC Health has 6000 total employees corporate wide with 39 at the data center.

GIAC Health's primary source of revenue comes from patient payments, and insurance reimbursements – from the private sector and state and federal government. The Information Technology department of GIAC Health has no direct role in earning any of the income of GIAC Health.

GIAC Health-IT has enterprise staff located at the data center, with 3 technical staff that visits the 3 hospitals and 2 long term care facilities on a regular basis. The purpose of the roving technical staff is to install, repair and maintain computer equipment at the 5 sites and to assist with questions regarding the office applications that are installed on the computers. The staff at the data center maintains the corporate office equipment.

The annual payroll for the GIAC Health -IT is $ 2,932,000.00 and is broken down in the following:

o Network Administrators	6	$450,000.00
o User support staff	6	$300,000.00
o Help Desk	4	$183,000.00
o Regional (roving) staff	3	$225,000.00
o Operations	9	$410,000.00
o Office (application) support	2	$104,000.00
o Security / Disaster Recovery	2	$180,000.00
o General Staff	3	$150,000.00
o Directors	3	$630,000.00
o CIO	1	$300,000.00

.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

2.) Diagram and Description of GIAC Enterprises

The GIAC Health infrastructure is a rather straight forward design. Access to the system from the Internet is through a CISCO Perimeter router, a switch (with one for failover) and then through the Cisco Pix Firewall. We have implemented a failover firewall in case of failure. Upon clearing the firewall and another switch then access to the internal network has been reached.

On the reverse, the internal network access to the Internet must pass through a Web Filter product that allows access to only sites approved by GIAC Health.

The private network has several application servers that are used by the Health System, file servers that hold the patient and financial information. Users at the hospitals, long term care facilities and the corporate office have desktop and laptop computers that are attached to the network.

Our Network has two DMZ's. One is for outside access – from our vendors that dial in through CITRIX or have direct VPN connection. Users that dial in from home can also use Citrix and those which have cable modems can use the VPN connection as well.

The second DMZ is for our Mail server and Web Server. These are connected through a router to the firewall.

Access lists control where individuals are granted access to and from the DMZ. Those that are given access from the outside can only get at those specific machines that are defined in the access control list.

We have intrusion detection in the first DMZ – as it poses the most potential for attack and we have IDS after the Firewall – to monitor any activity that might slip past the Pix boxes. The IDS is monitored on a regular basis by the Security team as well as the Wan team.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

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

The primary role of GIAC Health Information Technology is to promote, protect, support and improve the quality of GIAC Health through the equitable, efficient and cost effective use of information technology.

The office is responsible for the technical and user support as well as ensuring the integrity of the Medical Application. We support of the network and hardware at the facilities, update all hardware with virus and operating system updates and train staff on office product updates.

The office manager is the Chief Information Office and reports to the Chief Executive Officer.

The work in our office contributes to the revenue by allowing for fast and accurate admissions, timely lab results and accurate patient billing. This is done by keeping the Medical Application current with updates as well as keeping the network up and error free which also aids in fast response when critical patient information is required. Proper training of office products allows for the staff to be more productive, utilizing those products to their maximum.

The office has ownership and responsibility for all computer hardware that is throughout GIAC Health.

The Help Desk is responsible for taking all calls from the Medical and office users, recording their calls in a tracking system and assigning them appropriately. The Operations staff run backups, sends offsite tapes out, run daily jobs and monitors the servers and network for possible failures. The Network Administrators are responsible for the network, servers and PC's throughout the corporation. The Office Support team keeps the office suite current, and assists users with using those applications. The User Support group works with the medical application staff to train, answer questions and correct issues. The regional support team visits the three hospitals and 2 long term care facilities to work with the user's one on one. The Security and Disaster Recovery team are responsible for the protection of the corporations assets by monitoring the network, user access and have a plan for recovery from disasters. The General staff are made up of three employees – book keeper, administrative assistant and a building maintenance person.

The IT department for GIAC Health consists of thirty nine employees, which help the 6,000 GIAC HS employees. The company has seven locations, with the IT department located at the Joliet, Illinois data center. The total expense budget for the IT department is $8.5 million dollars of which $2.93 million is for salary expenses, $200,000 for training and the remaining for upgrades, new hardware, and software expenses. GIAC Health earned just over $750 million from its patient care in the last fiscal year.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4.) Describe your Job Description at GIAC Enterprises

JOB TITLE: Security/ Disaster Recovery Administrator

PRIMARY DUTIES: The Disaster Recovery/Security Administrator is responsible for maintaining the highest level of security and would establish security measures to protect confidentiality of data, insure appropriate access and assist with internal controls to cost-effectively protect Information Services assets from intentional or inadvertent modification, disclosure or destruction.

Will provide reports to superiors regarding the effectiveness of data security and makes recommendations on the adoption of new processes and/or procedures.

Measure of Success: Regularly scheduled audits that show GIAC Health is up to date on all Federal, State and local laws, JCAHO standards, HIPAA regulations or other regulatory agency requirements which apply to the assigned area of responsibility and ensures compliance with all such laws and regulations. In addition, technical audits will also be performed to identify the status of the network.

SECONDARY DUTIES: The Disaster Recovery/Security Administrator is responsible for developing, testing, implementing and maintaining policies and procedures to protect the data, activities and physical assets of Information Services. The Administrator directs the disaster recovery process and the use of offsite storage locations and resources needed for recovery

Measure of Success: Having annual disaster recovery tests with documented result and plans of action for the next test.

Salary:
- One hundred thousand dollars

Direct Supervisor:
- Chief Information Officer
- Corporate Risk Manager

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

5.) How does GIAC conduct its business?

The flow of business starts when a patient is admitted to the facility. Required information is gathered on the patient, which is stored in the Medical Application. This information is shared between the different departments within the facilities. The Medical Application is vital to the successful treatment of the patients as all pertinent information is stored in this application. The information is viewed by doctors, nurses and various departments that are required to treat the patient.

The orders are submitted by the appropriate staff and doctors on the floors for the patients (customers). This information could include orders for drugs that are then sent to the pharmacy for filling, or testing that is required by the laboratory. These orders could also include a treatment – physical therapy, inhalation therapy or an x-ray. In addition, these orders could also be sent to the cafeteria regarding special dietary needs for the patient.

The Medical Application sends the appropriate orders to the departments so that the pharmacist knows that medicines to send to the floor; the lab knows what tests to run, and where to send the results as well as the cafeteria being able to create an appropriate meal for the patient that will not adversely effect the patients condition.

The departments then send the requested drugs, meals, supplies or medical staff to administer the required procedures to the patient's room. The system also reduces the inventory for medicines and other supplies that were used for that patient. When a certain inventory level is met, a purchase order is created and sent to the corporate purchasing department notifying them to replenish supplies.

All charges that are incurred during the stay are added to the patient's bill. These charges are tracked and reported in the Medical Application.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

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

Those business partners that have signed an agreement with GIAC Health systems gain access to those areas via the DMZ1 (CITRIX dial-up and VPN). Each partner is only allowed access to those servers and applications that are required to complete their work. These partners include Medical Records staff, doctors and the vendor's software support team.

Once through DMZ1 the path is through the PIX firewall before granting access to the internal GIAC Health System. Access lists control where the business partners are allowed.

Our customer base does not need access to our systems, however if they need their medical information, they can visit the Medical Records department. They do have the ability to access our Internet site, which is housed by a third party.

The suppliers are notified via electronic purchase order when supplies hit a re-order point from the Health Systems purchasing module.

The GIAC Health Staff are connected to the infrastructure at their work stations. Employees are given access to the Company Intranet, Internet and E-mail depending on their job.

Each medical staff employee is matched with a pre-defined user profile that allows them access to only those areas necessary to complete their respective tasks/inquiries. Nurses can not see payroll data, and the accounts payable person can not access lab results.

Those IS staff that support the Clinical Health Application do have access to all areas of health application; the financial support team can not see any patient related detail.

The IS technical staff has access based on their job to servers, routers, the firewall, web access controls and other hardware and software necessary for support.

The security staff has access to exception reports from the IDS, web filter, e-mail and the Health Application security reports. Regular audits are performed.

Remote staff can dial in using CITRIX or VPN through there ISP. They can also check their e-mails from their ISP using Outlook Web Access (OWA). All of which is controlled through the user profile previously defined based on job descriptions.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

All staff can access the company Intranet using their sign-on at specific locations in the hospitals and long term care facilities. They can also access the Internet at secure terminals in Human Resources. Because of their specific job requirements, not all staff are given e-mail.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

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

The “crown jewel” of the GIAC Health Care Corporation is its patient database. This database consists of the following components:

- Patient Database
- Results Database
  - Lab Database
  - Medical Records Database
  - X-Ray Database
- Financial Database
  - HR/PR Database
  - Financial Database
- Reporting Database

This information is stored on file servers that are located in the corporate data center. Access to the data is controlled by the user’s profile – which allows only access to required patient data. These profiles are defined by job type and level within the entire GIAC Health enterprise.

All patient data is governed by recently passed HIPAA privacy and security regulations, requiring GIAC HCH to assure that access is restricted and that proper security controls are in place at all times to monitor the access.

The patient information is stored on the Medical Health System. This information is accessed by those staff that is given access via their profile to the specific areas required by their job function/description.

The Medical Health System application is maintained by their own support staff. The user support staff is the first line call. They assist users with questions and contact the Medical Health Systems support staff if necessary.

All data on the Medical Health System is backed up on a daily basis and at such time, two tape backup copies are created. One copy remains on site and the second copy is sent to our off site vendor.

Contracts for purchased goods (medical only) are maintained by the corporate purchasing department. By ordering corporately, the organization saves money. All computer related purchases for the entire organization are made by the GIAC Health Information Technology department. This also allows for volume purchase savings, proper inventory levels, and standardization of all hardware and software running in house.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

This information on all purchases, contracts and purchasing contacts is stored in the financial component of the Health System. Those users that have the appropriate access via their profile can see the agreements, inventory, etc.

All GIAC Health employee information is stored in the HR/PR module of the Health System. This information is updated by the appropriate Human Resources or Payroll staff person at the sites or at the corporate office.

All written information is kept by the Human Resources department in employee files at their respective location.

Access to the staff information is available to each staff member's manager, the human resources department, payroll department.

Another crown jewel for our organization is our budget tracking and forecasting system.

This information is stored on a server with access granted to the financial officers and some team members. This system is maintained 100% by the vendor. IT has no ownership of this system, hardware or software.

The information stored on this machine is used to forecast staffing, capital improvements and the corporations long term financial plans. Also stored in this machine are the current corporation financial data.

This information could cause many issues if it were viewed by unauthorized staff or financial institutions, vendors, news agencies or competing health care organizations. Some of the issues could be a change in the financial rating of the corporation – resulting in higher interest rates, or lower bond rating as well. If prospective patients see this information, they might choose to go elsewhere because they would be afraid of reduced staff and poor service. Doctors might not want to be associated with the organization because of the financial condition of the organization or they make unreasonable financial demands of the organization.

If competing health care organizations found out the growth plans, they could alter theirs to get a jump on the market.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

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

The “crown jewel” of the GIAC Health Care Corporation is its database and identified into four main jewels:

- Patient Database
- Results Database
  - Lab Database
  - Medical Records Database
  - X-Ray Database
- Financial Database
  - HR/PR Database
  - Financial Database
- Reporting Database

For computer and network access, employees could access the patient database using report tools that are designed to create lists of patients in the hospitals used by clergy and volunteers. This would show them who is in the hospital, room numbers and what the initial diagnosis of the patient is. Employees that would see this information would have knowledge of our patient’s confidential medical information and could spread this information in the community. This could be potentially damaging to someone that might not want their condition known, as it could cause harm to their family or business. The inquisitive employee could also sit down at another employee’s computer that has the correct access level to the patient database and find information that they desire.

A staff member wanting to gain access to the results database would use the same techniques as described above for the patient database. The results database has much more sensitive information - the tests that were ordered by the doctor and the results of those tests. The motivation is also the same.

If an employee were to access the financial database, they could see information similar to what would be found on any organization annual report. This could cause severe damage to the well being of GIAC Health. If competing health care organizations were to find out, they could use this information to damage GIAC Health in the patient and financial community. If information about terms and conditions of contracts we have with vendors were released, it could potentially cause GIAC Health to be in a weakened position during contract negotiations. The employee could also sell the information to a competitor giving them unfair advantage during contract bidding. The potential for revealing salaries, benefits and perks for management can cause moral issues within GIAC Health.

The reporting database has the potential to be the access point that will yield the most information about the patients in our facilities. As the report writers get easier to use, the ability to create reports that show information is easier as well. The report writer has

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

access to all patient information, human resources and payroll as well as the financial data.

Non computer related threats would affect all “four” of our crown jewels. We are in an area that is very susceptible to violent storms. Tornados and lightening strikes are very real concerns for our offices. The tornado could severely damage our data center, which would cause the “crown jewels” to be inaccessible for a period of time until the disaster recovery plan was exercised. Lightening strike could also cause machinery to be damaged thereby causing issues accessing the information. Anytime that you are in a “disaster” mode, security can become lax in the ensuing confusion. Recovery tapes, reports and other protected information could be easily removed and used by anyone in or outside of the organization.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

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

We are a health care facility that has public access 24 hours a day. Anyone within the hospital or long term care facility could gain access to an area that is unoccupied, or could use computers that are in an open area to access our patient database. Scenarios of possible access would be using the report writer "wizard" and creating a report on recent admissions. This report could be copied to a diskette or burned to a compact disc. The report could also be attached to an e-mail and sent to the person for further use.

Though tedious, screen prints of patient admissions could also be created.

In addition, reports, charts and other sensitive information that might be left on an unoccupied desk or unlocked office could also be looked at or removed and copied.

With this data, the person could sell it to drug manufactures so that they could solicit the patients to use their particular drug or product. This information could be sold to insurance companies, which in turn could increase their patients' insurance premiums. Financial institutions could use this information to deny credit to a customer because he or she might have serious medical conditions. It could also be used by potential employers to keep from hiring someone, or for current employers to deny a promotion. The person that gained access could also use the information as blackmail (for the above reasons) to the patient – especially if the patient was a prominent member of local society, or an elected official.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

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

BugBear virus is just one of the many malicious code viruses that exist today.

The BugBear virus is a mass-mailing worm that also spreads through networks, according to an article in Computerworld magazine. It can infect executable files and is particularly dangerous because it can log keystrokes on a user's computer, potentially giving personal information and account numbers to an attacker. The virus also contains backdoor capabilities and can shut down antivirus and firewall programs.

Thought the BugBear virus has primarily targeted the banking community, this worm could also go after our financial database “crown jewel,” allowing for access of financial information such as credit card numbers, bank account numbers, trust fund, insurance and other sensitive patient financial information.

The potential harm to GIAC Health would be the first and foremost loosing the trust of our patients and residents. Second would be the loss of our physicians.

Both of these would be devastating to GIAC Health. The medical community is very competitive these days and if the public were to feel that their financial information was being breached, they could also believe that their private patient information was in the same jeopardy. They would not want to be admitted into our system, which would cause us extreme financial problems. The reduction of patient days will increase the “low census” days off, which intern can lead to layoffs. Reduced staff could cause for a decline in patient care, further leading to patients going elsewhere for better patient care.

If the patients were to utilize other medical facilities, we could also see our doctors depart because their patients were going elsewhere for medical care. If the physicians are practicing at other facilities, they would be more likely to suggest those same facilities for follow-up care, which would increase our financial loss due to declining new and returning patients.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

11.) Identify the most severe threat.

Our organization needs to provide fast reliable information to doctors, nurses and other medical staff that are trying to treat a patient. Time is of the essence. Our biggest threat would be a virus or worm that would cause our network to significantly slow or crash. For us, the threat would be the spread of the nachi/blaster worm.

This threat is very likely to occur. An e-mail virus that gains access to our system which spreads icmp pings. These pings kill the network bandwidth thus slowing network traffic.

Transcriptionists that work from home on their home pc's do not have current patch levels nor do they have up to date virus systems. They could very easily spread a virus throughout our entire organization.

The potential damage to our organization is catastrophic. Test results can not be viewed or sent to the doctor. A nurse on the floor can not get to the online chart to see what the doctors' orders are. A pharmacist would not know that an order was needed for the patient, or would not know that the patient was allergic to a particular medicine.

If the system were down, then all important information would not be available to the medical staff. The ability to properly treat patients would be greatly reduced, and could lead to misdiagnosis or even death. At a minimum, the ability to function efficiently would be reduced.

No matter how careful we are, something like this could even affect our backup tapes. We must use extra caution if we were to restore or declare a disaster and go to our hot site. A thorough system check must be completed in this instance prior to opening the system to our users.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

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

The strategy defined to stop the open access points from our dial-up and VPN users would be to implement the CISCO remedy called Cisco Trust Agent. This product, which is installed on laptops and home computers, will collect information on those machines that are attaching to our network. When the device tries to attach to our network, non compliant devices would be denied access to our network, issuing a message to the user explaining the reason for denial. Depending on the setup, the devices could be put in quarantine or allowed limited access to our network.

This process would take three weeks to properly put together the correct action plan of implementation of this project. Implementation (depending on availability of the hardware) would be 4 – 6 weeks.

Things to consider would be equipment required, licensing of the product, process to get this in place, a policy that will indicate our new position and requirements for our vendors, VPN and dial in users. Also needed to be considered would be projects in progress and projects already scheduled to avoid staff being overbooked.

This project will require a project leader to create the project, assemble the required staff and keep the project moving.

Technical staff (4) will need to be involved – one from the security team, one from the network group, one from the user support team and one from the help desk.

The security staff will need to have knowledge in the Cisco Trust Agent and associated products (anti virus).

The Network staff person will need to know the layout of the networks so that the device(s) can be properly installed and configured.

The user support team person will be there to help with notifications to staff members of the upcoming changes to dial-up and VPN.

The Help desk person will be available to take calls and provide solutions that were created by the Security, Network and User support personnel.

We would need to purchase the Cisco device that will be plugged into the network and the Cisco Trust Software. There will be no additional staff costs as this calls for no additional FTE's. The cost of this security measure would be limited to the price of the Cisco device and software.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

13.) Review the backup strategy

- High level approach that you recommend, backup to a department server, connect to USB port with portable drives and be certain to explain your reasoning.
    - This would be a very time consuming task to manually backup each local drive on every desktop and laptop in our office using the USB
    - This task is also subject to failure – especially if the people designated to performing the backup were gone/ busy / quit
    - The best approach would be to backup the shared C drive on a backup department server, and then backup the entire server
- List software product(s) needed to support your recommended approach and their cost
    - A reliable product like Legato $1,768.75
- List hardware required to support your recommended approach and their cost
    - DLT8000 tape drive $1,450.00
    - Backup Server $2,190.00
    - Tapes
- Describe how these supplemental backups will be protected since all of your office's data will be on those backups
    - These backups will be added to the offsite storage plan – either by using an offsite company or by using the plan to store tapes at a nearby facility
- Including employee time to implement this solution, what is the cost of doing this for the first year?
    - By doing the share drive backup, once the process has been created and is in production, the employee involvement should be minimal
        - Implementation Time
            - Create the Legato backup process 3 weeks
            - Update security on all machines to share the "C" drive for Legato 2 weeks
        - Operations Time
            - Tape Changes and placing in bins 24 hours
        - Costs
            - Hardware $3,640.00
            - Software/License Fee $1,768.75

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

14.) Review offsite backups.

The high level approach to offsite back-ups would be to send the daily, weekly and monthly tape copies to an offsite vendor for storage.

One time tasks that are required would begin with researching available offsite vendors. Compare their costs for picking up and delivery of offsite tapes as well as the cost for "emergency" deliveries and at Time of Disaster. It should also be researched as to the time frames for emergency and at time of disaster deliveries. Find out what type of insurance the offsite provides to guarantee the security of your back-up tapes. Finally, what happens if the recovery is done out of state?

Research the cost of having a staff member take the tapes to another facility each day and the likelihood of it happening on a regular basis

Repeating tasks

- Nightly creation of the daily offsite tapes
- Placing the tapes in the bins for pick-up
- Returning those tapes that come back from the offsite into the production run
- If the decision is made to do the offsite tape storage in-house, the daily transportation of the tapes to the offsite facility

With a vendor, a signed security agreement that states they will not open the bins or do anything with the tapes they take offsite. You could also do a walk through the offsite facility to ensure that the bins are being stored correctly. Have the vendor provide references and do a complete background check.

For in-house offsite, locks would have to be placed on the bins to prevent unauthorized access.

There are several safeguards that will ensure that the data that you are storing offsite is not being tampered with. You can put locks on you binds, check at the site to be sure the bins are stored in a locked secured area and that the area has 24 hour a day camera surveillance. A confidentiality agreement with the vendor must also be signed.

The contract that you sign with a data offsite vendor is the availability safeguard that will ensure your tapes will be delivered when needed. The contract will state the amount of time it will take for the return of the offsite tapes to the data center.

For in-house, we would need to be sure that several people know the process, where the tapes are stored and have appropriate clearance at the offsite location, keys necessary to gain access to the secured site and to the bins.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

To validate the process you should conduct annual audits of the vendor site. Check to see that your bins are being stored in a safe and secure area. Have the vendor bring all your bins to an area for review – checking your inventory lists against the bins that are brought out during the review.

Also, stage an annual test of the return process – either to the data center or you could also have them sent to the hot site during one of your disaster recovery tests.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

15.) Devise a guerilla business continuity plan

The high level continuity plan will show the GIAC board of directions the need for a proper, appropriately funded Disaster Recovery / Business Continuity plan. For this plan to be accepted, the following will need to be brought to the attention of the board:

- Show costs (short and long term) of the plan
- Show what could happen if there is not a plan
- Show them regulations that require a plan
- Show them timelines of recovery

The most difficult task for continuity planning is to get a decision on budget dollars for this process. This is a very expensive insurance policy that hopefully will never be used. Also key to the successful start of this process will be the buy-in from the board and most importantly all levels of management within GIAC Health.

What are the repeating tasks?

- Testing the plan on a regular basis (at least annually).
- Revising the plan after the previous test.
- Expanding the plan to cover all of GIAC Health.

The best audit will be to have regularly scheduled continuity/recovery plan tests. Use the outcome from the tests to prepare for the next test. You should involve different staff members during the test – and have them follow the documented recovery plan that was used and updated at the previous test. This plan should also be part of a regular information technology audit.

The biggest mistake in trying to scale this to cover all of IT operations would be to try and recover everything from the get-go. This approach will not work as the scope of the project will be too large to properly address. Take small steps and set achievable goals.

Create a disaster recovery plan in two parts. First, you protect the “crown jewels” of GIAC Health. The plan will be structured to recover the mission critical medical application and have those systems available within the agreed upon time frame.

Second, other applications as E-mail, Internet, Problem Log Tracking, Budget Forecasting, etc. can be restored and brought back up.

Once the recovery plans have been devised and tested, a better business continuity plan can be created to cover all of GIAC Enterprises. Knowing how long a system will be down will give that area the ability to create downtime procedures in the event of a disaster with incremental steps dependent on the degree of the disaster.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

References

Newest BugBear virus targets financial institutions. Computerworld, June 11, 2003
http://www.computerworld.com/securitytopics/security/virus/story/0%2C10801%2C82015%2C00.html

Cisco, antivirus companies team to battle worms. Computerworld, November 18, 2003
http://www.computerworld.com/securitytopics/security/story/0,10801,87282,00.html

Cisco Systems news release, November 2003
http://newsroom.cisco.com/dlls/prod_111803d.html

US21 Computers, Inc. Alexandria, Va.
http://www.us21computers.com/osb/itemdetails.cfm?ID=489

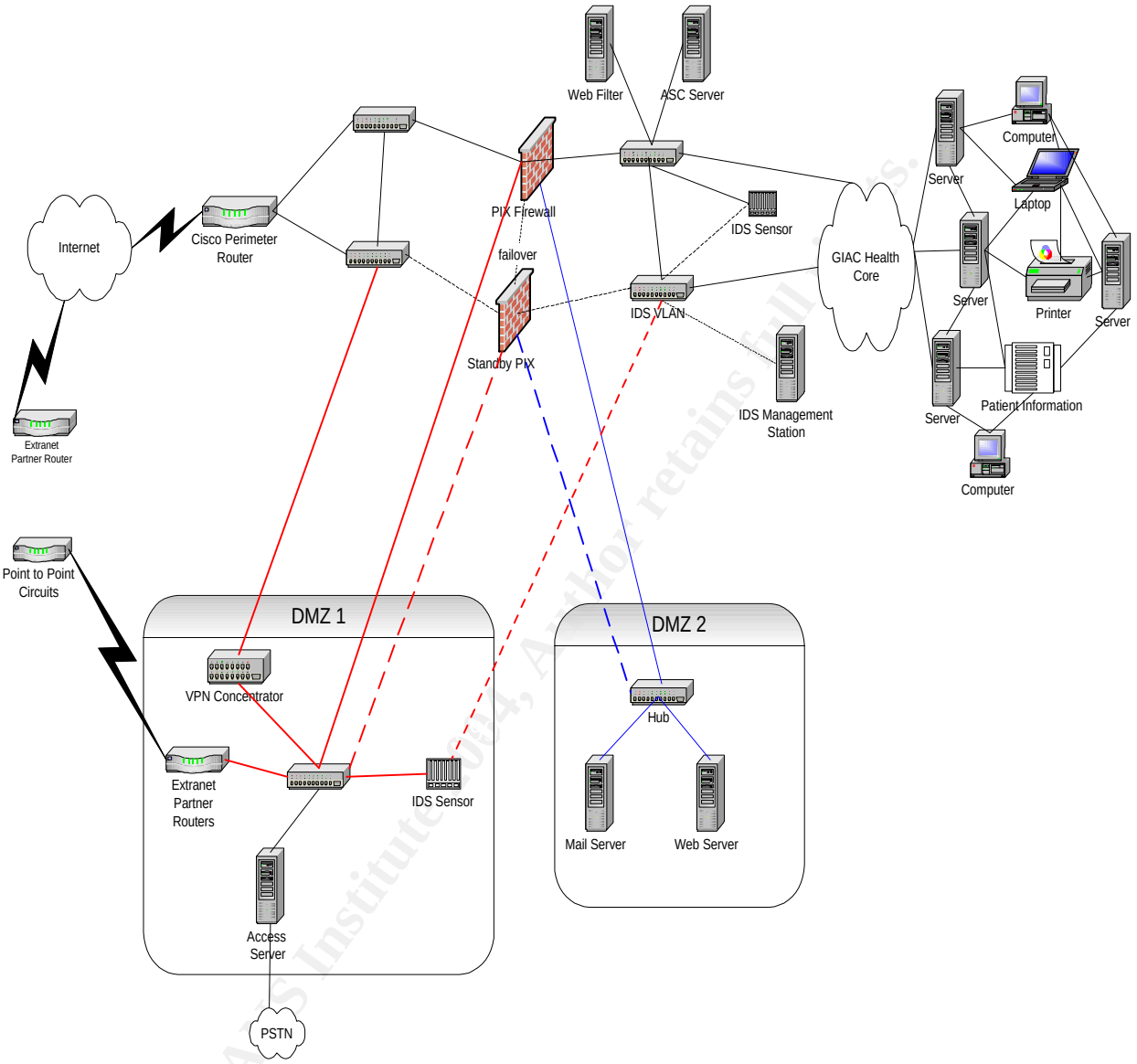
Pacific Data Storage, Inc**.**
http://www.pacificdata.com/dlt_tapedrive.html

NexTag / Page Computers
http://www.nextag.com/Legato_NETWORKER_SERVER_FOR~2520260z0znzzz1zzLegato_Networker_Networkzmainz2-htm

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

GIAC Health Network



© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.