Global Information Assurance Certification Paper

GIAC CHILDREN HEALTHCARE

GIAC Information Security Fundamentals + (GISF)
Basic Practical Assignment Version (v.1.0)

Matt Hoffman
Submitted on September 20, 2004

Abstract

This paper is written about a fictitious corporation known as GIAC Children Healthcare. The author is attempting to achieve a GISF certification. The first requirement was submitting a practical that shows his ability to improve the state of practice of information security.

Table of Contents

1.) Description of GIAC Children Healthcare

GIAC Children Healthcare (GCH) is a private non-profit corporation, whose main intent is arranging healthcare insurance for Maryland's uninsured children. GCH was created approximately fourteen years ago by Maryland's legislature due to the overwhelming amount of children without health insurance. The corporation serves the children only from the state of Maryland. The corporation is not a HMO provider but rather a facilitator. GCH maintains contracts with medical and dental providers to provide insurance for the children enrolled in its healthcare program.

The corporation receives its revenue or funding from the federal, state, and local governments. In addition, the enrolled families pay a premium of either $15 to $20 a month based on income guidelines. The most substantial portion of funding is from the state and federal government. In total the corporation receives approximately $350 million dollars a year to insure roughly 300,000 children.

The Information Technology staff does not contribute in anyway in earning that revenue. However, the IT department does monitor third party contracts that collect the premiums from the families. The IT department makes projections and cost analysis's to make a baseline for how much funding it will need to keep the corporation functioning in a proper and secure manner.

GIAC Children Healthcare is located at one site in Baltimore, Maryland. It leases an entire second floor of office space. GCH contracts out nearly all of its services with a third party administrator, HCI, Health Consultants Incorporated. HCI is located in Annapolis, Maryland. HCI has a 20,000 square foot facility which includes the main call center. The work done by GCH is mainly the administrative duties while HCI performs the grunt work.

GCH has approximately fifty employees, forty full-time workers and ten part-time workers. HCI has 110 full-time staff that work directly with the contract associated with GIAC Children Healthcare. On average GCH pays $1 million dollars a month to HCI. GCH's staff's payroll is approximately $1.1 million dollars. The following is the salary range for the fundamental positions:

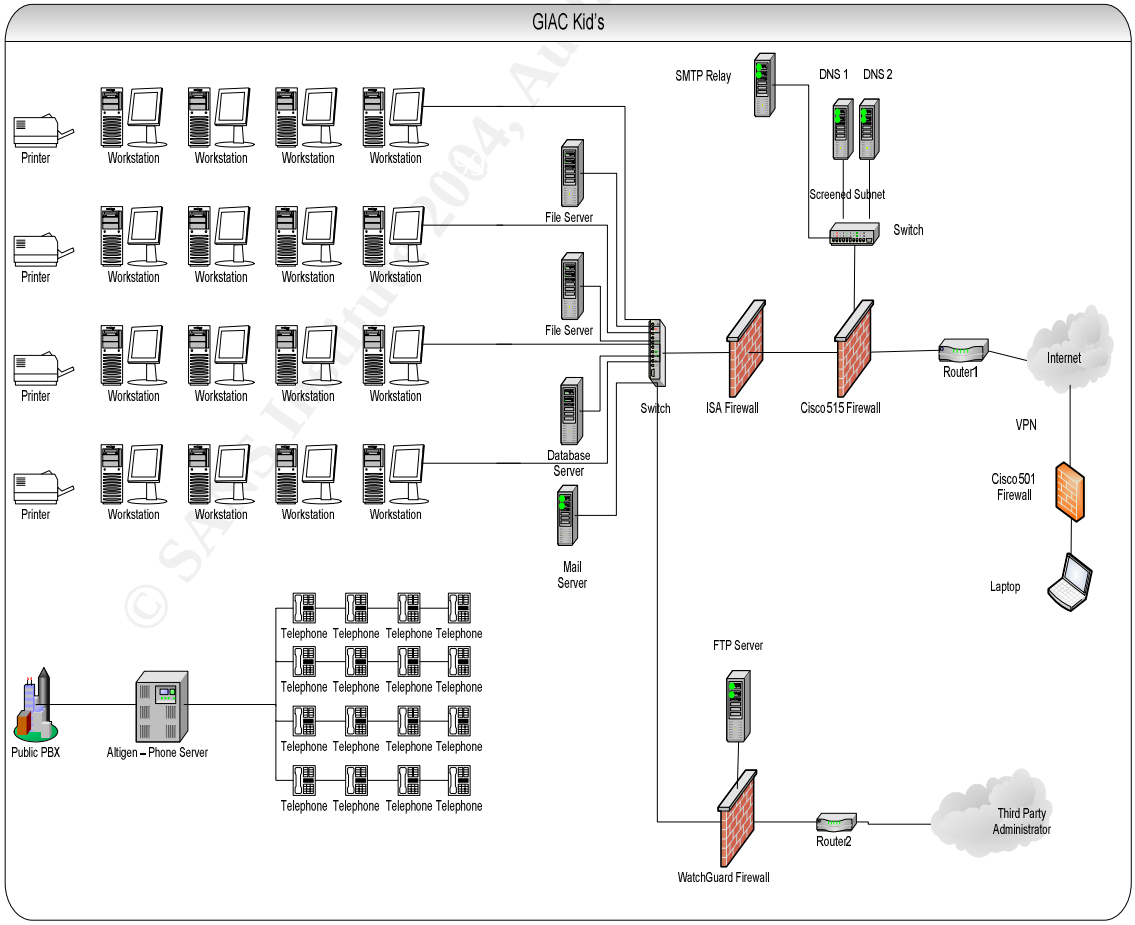
Executive Director -	$100,000
Deputy Director of Finance -	$75,000
Deputy Director of Operations -	$75,000
Division Director – External Affairs	$60,000
Division Director – Programs	$60,000
Information Technology Manager -	$50,000
System Administrator -	$37,500
Cash Management Specialist -	$37,500
Human Resource Officer -	$35,000

2.) Diagram and Description of GIAC Children Healthcare

GIAC Children Healthcare has a fractional T1 at its location. AT&T is the internet service provider. The ISP configures and monitors router1. GCH's first line of defense is a Cisco Pix 515 firewall. The Cisco Pix 515 firewall has three interfaces which are the internal, external and screened subnet. The internal network is the dot 1 network, its core protection is Microsoft's Internet Security and Acceleration server or ISA server. ISA server acts as a proxy firewall. In addition it also serves as a VPN server. The firewall located outside the office is a Cisco Pix 501 which forms a secure VPN tunnel with the Cisco Pix 515 firewall. The client uses Microsoft Windows 2000 VPN Client to get access to the internal network. Inside the ISA server are the remaining client machines, file servers, database server, and mail server.

The screened subnet has the SMTP mail relay machine and the DNS servers. GCH has a frame relay connection with HCI. The WatchGuard firewall also has a screened subnet. In this subnet the FTP server sits.

GCH does not host a web server. The web services are contracted out to Net Studios in Baltimore, Maryland.



3.) Describe your office, or department at GIAC Children Healthcare

The Information Technology Department mission statement at GCH is “to provide support and services that would enable the corporation to successfully function in a secure manner.”

The IT department at GIAC Children Healthcare consists of four full-time employees. The four full-time employees are the IT Manager, Security Officer, Systems Administrator, and Support Technician. The IT Department is responsible for configuring, maintaining, securing, and supporting all hardware and software purchased by GCH. The department keeps an inventory of all tangible assets. IT department is aware of who is in possession of what equipment, whether it be a laptop, desktop, or monitor.

The IT department at GCH has an annual expense budget of $225,000. This budget is estimated in the prior fiscal year by the Information Technology Manager and the Deputy Director of Finance. The IT Manager estimates the budget based on current and future projects, and the prior year’s budget. The Deputy Director of Finance requests the IT Manager to review current pricing for services that the IT Department manages. For instance, web server hosting, internet service provider, etc. However, the monies used for these services do not come out of the IT department’s budget. The IT department has a policy to purchase 25% of the total workstations a year to keep equipment from becoming obsolete. The budget can be broken down into a number of different buckets. A total of $10,000 is allocated for training and travel expenses. The IT Manager sits down with each IT staff member and discusses the goals and areas of interest with his employees where they would like to continue their education. The training can consist of a one day course to a full week course dependent upon recommendation of the IT Manager. If additional funds are needed they can be requested. Approximately $158,500 is associated with the salaries of the employees of this department. The rest of the money is used for equipment, software, licenses, and support contracts. IT department does not contribute to any revenue of the corporation. However, IT department keeps operations in tact which allow GCH to function. There is no comparison to earnings of the company since the corporation is non-profit.

The Information Technology Manager reports directly to the Deputy Director of Finance. The IT Manager is responsible for designing, configuring, maintaining, and securing the network. He reviews logs; monitors web activity, writes queries, and purchases new equipment. His duties also include managing the Systems Administrator, Support Technician, and Security Officer.

The Systems Administrator supervisor is the Information Technology Manager. The Systems Administrator is responsible for documenting, monitoring, maintaining, and configuring file servers. He is also in charge of all anti-virus applications, the phone system, and supervising the Support Technician.

The Security Officer reports directly to the IT Manager. The Security Officer duties include writing policies, analyzing the security and procedure flaws, and acting as a backup to the Systems Administrator.

The IT Support Technician reports to the Systems Administrator. The Support Technician primary responsibility is handling technical support for the employees at GCH. The Support Technician is usually the first point of contact for employees at GCH. The Support Technician usually hears of problems via phone or email and solves them using the same form of medium. If necessary he will visit an employee's workstation and diagnose the problem. If he is not able to resolve the problem he will relay the issue to his supervisor.

4.) Describe your Job Description at GIAC Enterprises

The Security Officer salary is $40,000 a year and reports to the IT Manager. He is a member of the IT department. The Security Officers job is divided into two main responsibilities.

The primary responsibility is handling and accessing the security at GIAC Kid's. In some ways this is a joint responsibility with the Information Technology Manager. The IT Manager has a better understanding of the networking and acts a secondary mind when analyzing the defending the network perimeter. The Security Officer will analyze the network, server, and workstation configurations and make recommendations with either the Systems Administrator or IT Manager. Together they will write polices and procedures. The Security Officer is an expert on HIPPA, and is up to date on the latest technologies that involve security. He also is responsible analyzing a third party administrator's operations to see if they are up to par with today's security standards. He and the IT Manager travel to HCI on a yearly basis to evaluate their security in person.

GCH believes in continual education of its employees. The security officer will be sent to training throughout the fiscal year. The security officer will attend SAN's and other security conferences and maintain certifications that are offered in his area. Bi-annually GCH will be audited by a top professional security firm that will access and diagnose the weak points and strong points of the corporation's security focus. Throughout the audit the Security Officer, IT Manager, and Systems Administrator will adjust certain procedures and network infrastructure to get approval from the consultants who did the audit. The audit will be discussed with the CFO and IT department. After reconfiguration and adjusting certain techniques and procedures the CFO, IT department, and auditors will go over the remedies and make a final conclusion about the security of GCH.

The secondary responsibility is technical support. The security officer's role is primary to be the backup for the when the Support Technician or Systems Administrator is either not in the office or is overburdened.

The Security Officer is evaluated and critiqued yearly by the IT Manager.

5) How does GIAC Children Healthcare conduct its business?

GCH's main focus is administering the program. Most of the grunt work is handled by the third party administrator, HCI. However GCH constantly monitors HCI for quality assurance by auditing, establishing and maintaining contracts, and housing the grievance department for the program.

When families apply to the program they fill out an application with a $20 application fee and submit it to the corporation. HCI receives the applications scans the application to a .tiff file and enters it into a database. The .tiff files are zipped and PGP encrypted. The image files are then placed on the GCH FTP server. The IT Manager decrypts, unzips, and places the file on a file server. One of the audits GCH performs is monitoring the accuracy of the data that is entered into the database.

Another key element is monitoring the program to make sure that all the automated functions are performing in the correct manner. Since GCH is funded primarily by state and federal government, changes to the program are quite frequent. GCH makes sure the changes are applied to the proprietary software built by HCI. Employees at GCH verify that data in the database is in proper location and show the correct information.

Each family must either pay $15 or $20 per month to have coverage each month. The families can submit the payment over the phone by calling a toll-free number or through the GIAC Children Healthcare web site. GCH contracts out the payment services to Global Payment. There is a link on the web site that redirects the user to a secure web site that will process the payment. The family must pay via Visa or Discover and enter in their family account number. The payments each day are sent to GCH/HCI and posted the families account number. GCH must receive this payment by the last day of the month in order for coverage to be maintained. GCH does not host the call center, which also is contracted to HCI. It is essential that the web site, payment processing link, and call center are uninterrupted. There are built-in service level agreements in the contracts that both parties must meet or they will be penalized or the contract will be terminated. GCH has a unit that monitors and evaluates the call center at HCI. The employees at GCH have the ability to call from GCH to HCI to monitor, record, and barge in. A separate daily report sent from Net Studios and Global Payment via email is sent to the operations unit at GCH. The Operations unit monitors the associated service agreements.

Each month HCI performs a process that looks at all the family accounts and checks if they are eligible for coverage. The process is performed after the close of business on the last day of the month. After the process is completed HCI transmits an eligibility file to the different HMO's and a separate file to GCH. The eligibility file displays what child should receive coverage for the month. The HMO will than insure the child during the next month.

GCH will import the file into a database at its location and run a java based program that runs the file through multiple tables that finally calculates the money due to the HMO's. It is extremely critical that the databases at HCI do not go down. Call Center Representatives and employees doing grievance complaints always require access to research issues, make changes or assist families in other ways.

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

In order for employees at GIAC Children Healthcare to actively monitor the HCI Application and Call Center they need to have access to the database at HCI office. HCI and GCH have a connection using frame relay, GCH and HCI transmit all data excluding email via this line. HCI and GCH both maintain a firewall and router on each side of the WAN. GCH protects itself with a Watch Guard firewall. The firewall was configured by the IT Manager. The router is maintained by provider, Sprint.

GCH installs the proper software and if a supervisor states the application is needed for his or her employee to fulfill his or her job duties that software is added. GCH Security Officer requests from HCI IT staff that a login and password be created for an employee at GCH. The application that is installed is Child Healthcare Administration Database also known as CHAD. The application is Microsoft SQL on the backend and Visual FoxPro on the front end. Access permissions and restrictions are defined for each user account by GCH IT staff and relayed over to HCI.

Transmitting files between GCH and HCI are done over the private virtual circuit and routed to GCH FTP server which is located on its DMZ. FTP Server requires a login and password. The FTP server is administered by the IT Manager. Data that is transmitted between HCI and GCH that contains personal healthcare information also known as PHI is encrypted. GCH and HCI use PGP desktop software to encrypt the data.

Email is setup for all users of the corporation. Users are either restricted to internal or external email dependent upon their job duties. Each employee must read and sign the GCH Corporate Email Policy before he or she has the ability to use email. Microsoft Exchange Server is located on the internal network, while the SMTP Relay Machine resides on the screened subnet. The SMTP Relay Machine is protected by Web shield, an anti-virus application and the Exchange Server is protected by Groupshield another anti-virus application, developed by McAfee. Email is critical for the corporation to conduct business. Email has now become main form communicating in the business world. GCH must keep in constant communication with business partners, families enrolled in the program, etc.

Each employee has Microsoft Office 2003, VirusScan 7.1, and ISA Firewall Client installed onto his or her computer. The IT department created multiple custom installation types for Microsoft Office depending on what the supervisor states his or her employee will need. The basic install package includes Outlook, Excel, and Word. Other users may receive Visio, PowerPoint, and/or Publisher. The workstations are secured/hardened by the Systems Administrator using Group

Policy. Each workstation has its patches updated at 3:00 pm daily using a SUS server at GCH. The anti-virus dat files are configured to update unassisted.

Employees also may receive Lotus Approach. The corporation has various auditing and other eligibility databases. Access to these databases is granted via shared password and access control lists on the server. The end users however cannot edit or design the databases. In addition the databases are located in separate folders that are permission based. The passwords are given out per division director's request.

Internet access is granted by an employee's supervisor. If a supervisor thinks it is necessary for his or her worker to perform his or her job, they are given access. Each user with internet access must sign the GCH Internet Acceptable Use Policy.

The executive director of the corporation has a home office. The internet service provider at this house is provided by Comcast. Comcast has provided her with a cable modem and a dynamic IP address. She requires accesses to the file servers, email, and internet from her home. The connection to GCH offices is by Virtual Private Network or VPN. An encrypted tunnel is formed between her Cisco 501 and the corporation's Cisco 515.

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

The most integral crown jewel at the corporation is the personal healthcare information of the families that is stored on the HCI database and transmitted to GCH. The CHAD program has addresses, phone numbers, names, social security numbers, etc of the families that have been enrolled or are enrolled in the program. The information stored in this database is extremely sensitive. The information is accessed using the CHAD program. GCH users access this information by opening up the application and entering in his or her username and password. Employees can view the actual applications that were filled out by the parents when enrolling their children. The information is maintained by the HCI staff and cannot be changed by the GCH employees.

The next crown jewel is the contracts GCH has with the HMO providers. These contracts are offered through a bidding process each year that GCH conducts. The corporation offers any HMO in the state of Maryland the ability to bid for being an HMO provider on a per county basis. GCH requires a proposal and presentation. The proposal and presentation are graded by the External Affairs department and the board of directors. The contracts are proposed and reviewed by our External Affairs Director and an external legal team. The contracts are stored in a locked office in a filing cabinet. The External Affairs Director has a key to this office. The rates of the contracts for each county and HMO are forwarded to the IT department. The IT department takes this information and enters/updates the information into a rates table using Microsoft SQL Server. Microsoft SQL Server is a program loaded only on the IT Manager, Systems Administrator, and Security Officer’s computer. The IT Manager is the only employee with the permissions that allow him to update or delete information. The integrity of this data is critical because GCH uses this information to pay the HMO’s. After GCH receives the file from HCI on which kids are eligible each month the IT Manager imports this file into an expenditure table. He then runs the java program that creates multiple expenditure reports. The reports that are produced are quite detailed and are invaluable to the corporation. The Accounting department has read only access to these files. The corporation pays HMO’s based upon these reports.

Another crown jewel is the management information on each employee at GIAC Children Healthcare. The management information contains the salary information, performance reviews, and background investigations. The information is stored in the Human Resource Officer’s office in a locked filing cabinet. This office requires a key to unlock the door. The keys to open the cabinets are in the possession of the Human Resource Officer and her boss, the Deputy Director of Finance. The payroll information is stored on the network in a folder that can only be viewed by Human Resource Officer, Cash Management Specialist, and the Deputy Director of Finance. The payroll file is password protected. The actual physical documents that contain the salary of an employee are also stored in the filing cabinet. Supervisors in the corporation have access

to all information on their employees. Performance reviews are done yearly on employees by their supervisors. Depending on the funding that the corporation receives raises will occur based upon job performance evaluations and merit.

A fourth crown jewel that has not been mentioned is GCH check writing privileges. The check writing privileges are considered a crown jewel because of how the corporation obtains its funding. The corporation is audited by a private accounting firm, the Office of the Inspector General, and the Federal Government. If money is unaccounted for or does not have the correct mechanisms that protect it, GCH could have a significant price to pay. GCH has reputation to keep and failure to pay vendors on time could significantly reduce the existence of the program.

GCH write checks for expenses, to HMO's, but mostly to families who apply to the program but are not eligible. When a family applies to the program they must submit a $20 application fee. The application fee essentially isn't an application fee, but the first month's premium for the family if they would be become eligible. However, thousands of families apply to the program a year that are not eligible. If the families are not eligible GCH must submit a refund check in the amount of $20 and mail it back to them. Instead of using an electronic signature GCH uses a stamp. Upper tier management believes that a stamp is safer than electronic signature. The stamp has the Executive Director's signature on the stamp. In addition GCH uses pre-printed checks. The stamp is secured in a fire safe in a locked filing room. Access to the filing is by key, the Cash Management Specialist and the Deputy Director of Finance have keys to this room. The safe is opened via a key which is in possession of the Cash Management Specialist and Deputy Director of Finance. The Cash Management Specialist prints the checks on a non-networked printer located in her office and then stamps the checks. The Cash Management Specialist is the only person authorized to use the stamp. In addition the signature of the Executive Director can only be cashed up to $5,000. Another signature would be required to for checks that exceed this amount. The secondary signature is the External Affairs Director.

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

An employee at GCH could become disgruntled over his latest performance review and want to get back at the corporation by ruining its reputation. An employee who does not have access to the CHAD program could still obtain the sensitive information by visiting a fellow worker at his workstation while the information is on his or her screen. The individual could memorize the information and then write the information down. In addition the majority of workers at GCH insist on printing out documents and reviewing on a printout rather than on the computer screen. The printouts are often not picked up at the printers or done so at a later time. The printers at GCH are mainly all network printers that are shared with about a 10 employees to 1 printer. The employee could go up to one of the printers and take some documents that include an abundant amount of PHI and either sell the documents or use the documents to steal someone's identity. If news of this compromise would be leaked to the media the corporation's reputation would be devastated

GCH has multiple contracts with HMO providers. The actual physical contracts are stored in a locked room in an unlocked filing cabinet. There are only two keys exist for this room. The keys for this room are in the possession of the Director of External Affairs and the Administrative Assistant. The Administrative Assistant has master key for the entire office. The supply room is also locked. There are three individuals with keys to the supply room. They are the Administrative Assistant, Purchasing Coordinator, and Human Resource Officer. Usually an employee requests the key from the Purchasing Coordinator. However when the Purchasing Coordinator is not in the office, he or she usually asks someone else with a key. It is not out of the ordinary to ask the Administrative Assistant to use her key to get into the supply room. An individual could access the filing cabinet during lunch hours or while the office is empty and grab the documents and destroy them. This would leave the corporation with no physical documents of the contract or rates for the contract. The server that houses all the data on the contracts would be the second step for an insider to cause havoc. The IT Manager works in an open cubicle at the office. The IT Department uses Group Policy Manager in Microsoft Server to implement locking workstations after five minutes of no use. The insider may circumvent around the IT Manager's workstation before the close of the business day and wait until he leaves for the day. If the IT Manager does not lock his workstation manually the individual could maintain full access to this workstation if he or she reaches the workstation within five minutes. The individual could go into the SQL Server and change or delete the premium amounts. The motivation for an employee to do this is that he could be upset with either the IT Manager and decide to attempt to make him look incompetent. Also, his motivation could stem from an HMO that upset him. He or she could decide to change the premium amounts in order to cause confusion with monthly payments.

The Support Technician received a smaller raise than last year. The individual wants to know if this was corporate wide policy or if others also received the same raise. The data is on the network server in a folder accessible to the Cash Management Specialist and Human Resources Officer. The Support Technician decides he will change some of the information and mess up individual's paychecks. The payroll is done once a month and many of the workers uses an automatic withdrawal on the day they get paid. The Support Technician decides he will lower employee's paychecks which will cause NSF fees due to their automatic withdrawals. The Support Technician goes over to the Human Resources Officer and explains he needs to add a patch to her computer and it will take some time. At this time the Human Resource Officer leaves her workstation without logging off. The Support Technician accesses the folder that holds payroll file. The Support Technician quickly installs a password breaker in order to get access into the file. Once access is granted, he changes the salary and pay individuals are suppose to receive this upcoming month.

An IT employee is extremely dissatisfied with the salary he receives from GIAC Children Healthcare. He believes he should be paid much more money. The IT employee submits a medical reimbursement to the corporation and waits for his reimbursement check. The individual holds onto this check until the Cash Management Specialist begins to do refund checks. Once the Cash Management Specialist goes to lunch he asks the Administrative Assistant for the key to go to the Supply room and goes into the Cash Management Specialist office. The IT employee enters the office and grabs a few pre-printed checks. He then finds the stamp with the Executive Director's signature and stamps the pre-printed checks with the signature. Later that day he goes home prints out the checks with ranging up to an amount of $5000. He quits the corporation and deposits the checks.

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

The personal healthcare information of the children and families enrolled in GCH must be protected. It is one of the crown jewels of the corporation. If this information fell into the wrong hands it could be detrimental to the corporation. The corporation would lose its integrity and possibly its funding. An outsider would want this information so he could steal a person or person's identity. An outsider could use this information to commit identity theft.

An outsider threat vector for obtaining the PHI would be social engineering. An outsider could engineer his way inside the offices of GCH by getting job with the cleaning crews. During the cleaning crew shift the person would be privy to printouts of PHI that are left on employee desks, trash, etc. The corporation has a policy that all PHI documents must be placed in the shredder and are not allowed be left on one's desk. However this policy is not always followed. The individual could obtain just enough information from printouts found in the trash or on desks to have the ability to call up a GCH Call Center Representative and obtain more information. In addition the individual would have the ability to log onto an employee's workstation and try and access the CHAD program. It is out of the ordinary for employee's to leave passwords on post-it notes on their desk.

Once the outsider obtains this information it is only matter of time before he steals a person's identity or sells a person's identity to another individual. With continued occurrences it would be a matter of time before it could get traced back to the corporation.

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

A malicious code threat to any of the crown jewels or most of the crown jewels could be caused the W32.Sasser.b worm. "Unlike many other viruses the worm does not spread via email", the self executing worm spreads by exploiting Microsoft Windows vulnerability (McAfee).

> The worm spreads with no user intervention required. This worm scans IP addresses for exploitable systems, once a vulnerable system is found the worm exploits the machine by overflowing a buffer in LSASS.exe. It creates a remote shell on TCP port 9996. Next it creates an FTP script and the remote host and executes it" (McAfee).

The victim's downloads a copy of the worm and executes it. The workstation could possibly infect all computers because it scans random subnets. If the workstation or server is infected a system shutdown prompt will appear and the computer will continue to reboot (Symantec).

The impact on the corporation could be quite severe. Employee workstations could be down for several hours or possibly longer. The server that stores the payroll information or contract information could get infected. Interrupted service would take place and possibly affect the nature of the business. The database server could be out of commission for unknown period of time.

In order to disallow this worm a computer or server must be patched with a security update for Microsoft Windows (835732). "The vulnerability allows remote code execution" (Microsoft). GCH uses a SUS server to push patches out to computer and servers. However, before the SUS server pushes the patch out it must be approved by either the IT Manager or Systems Administrator. If one of them forgets to approve the update the computers and servers will be vulnerable.

11.) Identify the most severe threat

By far the most severe threat to the corporation is an unauthorized person obtaining the PHI of children and families enrolled in GIAC Children Healthcare. The threat can cause the most damage to the corporation because it can ruin the reputation of the corporation and cause significant damage to families. Identity theft is extremely costly to the victim. If identity theft increases considerably the media could potentially find out and bad publicity for the corporation could take place. The incident would most likely be caused by negligence at GCH. Jobs at GCH would probably be lost and lawsuits could be filed against the corporation.

This is most likely because there are multiple avenues where employees can be careless about PHI. Employees may include PHI in emails between business partners and within the internal network. If the email is intercepted within the external the PHI could be used to steal someone's identity. An outsider could obtain access inside the GCH network. He or she could set up "passive sniffing which is listening on the raw network device for packets that interest you" (Tech FAQ). The intruder might install software on a server that "searches for packets that contain logins and passwords" (Tech FAQ). The intruder could later revisit the server or have the packets emailed to himself. The intruder could potentially get the password the IT Manager uses to run queries from the database at HCI. He or she would then have full access to the all store information with an opportunity to copy it.

Intercepting emails containing PHI is probably a more likely scenario than the passive sniffing, however both could occur with devastating impacts on the corporation.

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

The IT Manager has requested a remediation strategy that would limit the probability of the most severe attack. The allocated budget for this project is approximately $25,000.

GCH is presently lacking any intrusion detection systems or IDS. IDS would allow the corporation to "detect a penetration of a particular system or network" (ITSC). IDS would likely yield the best results in fighting the severe threat of sniffing. The IDS configuration would be installed outside the network firewall and be configured to monitor specific services. An Enterasys Dragon Network Sensor Appliance would be an excellent addition to the security of the network. The Enterasys Dragon was selected because of its "ability to detect and stop misuse and attacks across the network" (Enterasys). GCH will hire a consultant to install and configure the Enterasys appliance. The consultant will also train the IT Manager, Security Officer, and Systems Administrator on how use the appliance. The consultant will be at GCH approximately two full days to complete the tasks. The time associated with implementing the IDS is approximately two full days for the entire IT department excluding the Support Technician. The implementation of the IDS is broken down below:

Enterasys Dragon Network Sensor Appliance -	$5700.00
Enterasys Consultant (includes expenses for two days) -	$2000.00
Two Full Days (3 Employees) x (8 hours) -	48 Man Hours

GCH current email policy prohibits sending email that contains personal healthcare information. However enforcing that policy is extremely difficult. In order to resolve this situation GCH will purchase a PGP Universal server. PGP Universal server will encrypt and decrypt all emails sent from the corporation. PGP Universal server automatically creates a public and private key pair for each internal user and keeps the end user out of the mix. PGPU can enforce its encryption policy by domain and gives the option on how the corporation would like the recipient to receive the intended email if they are not using PGP. PGPU also acts as a web server and allows the recipient to retrieve the message security using SSL. The PGP Universal Server will require GCH to purchase a new server, PGPU software, and to hire a contractor. The contractor will install, properly configure, and train the IT department on how to administer it. The total cost of this implementation is as follows:

Dell Power Edge Server 2650 -	$3000.00
PGP Universal -	$10000.00
Contractor (includes expenses for two days)	$2500.00
Two Full Days (3 Employees) x (8 hours) -	48 Man Hours

The total cost of implementing both of these projects is $23,200.00.

13.) Review the backup strategy

GIAC Children Healthcare has an organization wide policy that states employees are to store data only on network drives. However that policy is not followed or enforced. The IT Manager has requested a backup strategy that allows the IT department to store data that is on the local drives of employee workstations. The plan must work 100% of the time and be completed once a month. This job is supplemental to the already existing backup strategy.

The idea that is devised would take advantage of the existing knowledge of the hardware and software that is already in use to perform backups of the network servers. The plan entails purchasing Veritas Backup Exec 9.1 for Microsoft Windows server and additional licenses for the employee workstations. IT department would not have to purchase a tape drive because already has one. The only other hardware needed would be to purchase an additional fifty backup tapes. Veritas Backup Exec would enable the IT department to have a one-time implementation cost and not be a redundant task performed each month. The IT department could perform other job duties each month rather than being burdened by performing a monthly backup on 50 workstations manually. In addition, executing the backups in this matter will keep the end-user out of the mix and not take up any of his or her work time.

Under this plan all workstations are accounted for except for the Executive Director's home office. Each month a member of the IT department will travel to her house and backup her local drives manually. An IT employee will install Ghost software and backup the local drives with an external cd-rw. The IT department will purchase a spool of cd-r.

GCH will install Veritas Backup Exec 9.1 to the existing server that has the prior version installed. This server was chosen because there were no prior issues with earlier version of Backup Exec and this server has plenty of resources for this application run. The IT staff will then install a remote agent on each user's workstation which allows Veritas to perform the backups remotely.

The IT department will use its Quantum Super DLT 320 Tape Drive to perform the monthly supplemental backups. Four new jobs will be created in Veritas Backup Exec. The jobs will be entitled Monthly Backup 1-4. These backups will store all data from the mail and file servers, and also include the local drives from thirteen workstations. The size of the local drives on fifty workstations is too large for a single job, this is why it has been broken down into four jobs. Monthly Backup 1 will be performed the first weekend of the month, followed by Monthly Backup 2 the second week of the month, and continued so forth.

All the monthly backup tapes and cd-r will be stored in a fire safe located in the local area network room. After each monthly job is performed it will be deposited immediately in the safety deposit box. The Security Officer and IT Manager are

the only IT workers with access to the safe. The local area network room is only accessible by key. The IT staff employees with a key are the IT Manager, Security Officer, and Systems Administrator. Access Control Lists are setup so they allow the IT Manager, Security Officer, and Systems Administrator to restore jobs. The IT Manager only has permissions to delete jobs or overwrite jobs.

The costs and time associated with this project are as follows:

Veritas Backup Exec 9.1 (includes licensing for 100 workstations) -	$300.00
50 HP SDLT Tapes ($55 x 50) -	$2750.00
Install Remote Agent on Workstations -	Four hours
Install Backup Exec 9.1 (configure) -	Two hours
Install Ghost and Burn on Remote Computer -	One hour

14.) Review offsite backups

The current policy for storing daily, monthly, and yearly jobs is to deposit them in a safe. The fire safe is located in the local area network room. Also, all the passwords the IT staff uses are stored in the same fire safe. The fire safe requires a combination to open the door. The combination is known only by the IT Manager and Security Officer.

The following is a recommendation by the security officer to implement a plan that uses an offsite facility to store backup tapes. The off-site facility that is selected is Maryland National Bank. Maryland National Bank maintains the highest level of security. There is video surveillance and a full-time guard at the bank. GCH currently conducts business with Maryland National Bank and currently has multiple accounts with them. When researching a secure facility the Security Officer approached MNB to see what kind of facilities they had to offer. MNB offered a complementary safety deposit box to the GCH due to the business GCH creates for MNB. The vault at MNB is located beneath the ground and requires an individual to travel through two heavily locked doors. In order to open the safety deposit box a key by an employee at GCH must be used in conjunction with a key from an MNB representative. MNB will provide GCH with a sheet to be filled out that would state who is an authorized individual and is granted access to the safety deposit box. The individuals who are recommended to have authorized access are the Executive Director, Deputy Director of Finance, IT Manager, and the Security Officer. MNB will provide GCH with two keys to the safety deposit box. It is recommended that the keys be distributed to the Security Officer and the IT Manager. In order to be allowed to venture down to the vault a GCH employee must show photo identification and sign a sign-in sheet. The name on the photo id and signature are compared to the name on the initial sheet MNB provided GCH. The MNB representative will then escort the employee down to the vault.

GCH will store all yearly jobs, monthly, and weekly jobs in the safety deposit box. The IT Manager or Security Officer will visit the vault every Monday to drop off the latest weekly job and every Friday to pickup the tape for the upcoming weekly job.

All the daily tapes will be stored in the fire safe located in the LAN Room. The daily tapes will be stored here due to the fact the information available on these tapes may need to be immediately available. The time required to travel to MNB is not worth the opportunity cost. GCH will cycle through approximately 20 daily tapes a month.

MNB is conviently located within fifteen minutes of the corporation. It is not too close, but not too far away. If by chance a workstation's data is unavailable the backup tapes could be retrieved and restored within one to two hours. Maryland National Bank is opened 9:00 am – 5:00 pm Monday thru Friday. GCH has

basically the same business hours. Twenty-four hour access to the safety deposit box is not necessary for the corporation.

The Security officer will audit every monthly backup tape by restoring a sample of ten different files from seven different workstations and three servers before the tape is deposited at the safe. The Daily and Weekly jobs will be audited in the same manner every other week by either the Security Officer or the IT Manager. The logs will be reviewed by the IT Manager on a daily basis. Quarterly the Security Officer will take data that is in the safety deposit box and restore it. He will compare the data restored prior to the deposit of the tapes to data restored afterwards.

The Daily backup jobs are performed Monday through Thursday. The Monthly Jobs 1-4 are performed every Friday dependent upon which week it is. The Daily and Yearly Jobs primarily backup the same data. However the Monthly job backups everything the Daily and Weekly jobs do, but in addition the supplemental data located on the employee workstation's local drives.

15.) Devise a guerilla business continuity plan.

The Business Continuity Plan or BCP is designed to provide fast response and adequate restoration that would allow the corporation to continue in case of any unplanned disaster.

GCH identifies the database that stores all the information on contracts and health plan information is extremely valuable and needs to be a high priority when executing the BCP. The database needs to become operational as soon as possible. Loss of the database would leave the corporation in extreme confusion. Each month the corporation has to pay the HMO's based upon the data that is stored in this database. If GCH would go delinquent, three hundred thousand children could potentially lose health insurance.

Identifying who is on BCP Team is the first task that is developed. The BCP team is composed of the IT Manager, Security Officer, Systems Administrator, Director of External Affairs, Deputy Director of Finance, Deputy Director of Operations, and the Executive Director. The team leader for implementing procedures is the IT Manager, however upper management make the decision on whether or not put the BCP into effect.

The following are BCP steps in the event of a disaster:

1. If the event occurs after business hours the IT Manager will be notified by the Building Manager of the disaster and damage to the building. In the event that the disaster occurs during business hours the first priority is ensuring employees' safety. If necessary the building will be evacuated.
2. If the disaster is after hours the IT Manager will contact the BCP Team via phone and discuss with them the news and plan to meet the team at the Executive Director's house in approximately three hours. Before the meeting the IT Manager and Security Officer will assess the damage to equipment at GCH.
3. The Security Officer and IT Manager will report the findings on the equipment and make a recommendation on whether or not they should continue with the Business Continuity Plan and if the corporation will need to prepare an offsite facility. Upper management will make a decision. If the corporation elects to follow the BCP a press release will be issued by External Affairs Director stating plans and status of the corporation. The corporation will also inform all employees and business partners.
4. The BCP team will contact a real estate agent and get the current listings of vacant office space. The Director of Operations will pursue this matter and have leased space within 24 hours.
5. The IT Manager will begin purchasing equipment that is mission critical to the corporation and have in place within twenty four hours. If

transmissions need to take place between HCI and GCH they will resort to Federal Express until the network is up. The Systems Administrator will be contacting the phone company and the internet service provider.

6. The Security Officer will visit offsite facility to pickup the company's backup tapes and policy's procedures manual. The IT Staff may have to resort to Policy and Procedures Manual when installing or reconfiguring certain pieces of hardware or software. The Purchasing Coordinator will begin purchasing office supplies.
7. The Alternative site will be declared "live" when the backups are finished restoring and the servers are fully functional. The secondary site should be live within 48 hours from the time of the disaster.

This plan needs to be audited once a year to find out if the Business Continuity Plan works. The plan will be simulated by the BCP Team with a fictitious disaster that destroys Global Children Healthcare. All steps will be tested to see if the plan can happen within 48 hours. One of the most vital steps is making sure the corporation can get a hold of these different individuals. The corporation will however not purchase new equipment, but test the tapes on current servers. After the simulated disaster the BCP will be reviewed and recommendations will be made to improve the BCP.

List of References

1. Microsoft, “Microsoft Security Bulletin MS04-0411.” 13 April 2004. URL: http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx (3 August 2004).

2. McAfee, “W32/Sasser.b.” 1 May 2004. URL: http://vil.nai.com/vil/content/v_125008.htm (7 June 2004).

3. Symantec, “W32.Sasser.Worm.” 27 June 2004 URL: http://www.sarc.com/avcenter/venc/data/w32.sasser.b.worm.html (3 August 2004)

4. Tech FAQ, “What is Packet Sniffing.” URL: http://www.tech-faq.com/data-networks/packet-sniffer.shtml (12 August 2004).

5. Enterasys, “Enterasys Intrusion Defense.” URL: http://www.enterasys.com/products/ids/ (12 August 2004).

6. Information Technology Support Center, “Best Practices - Intrusion Detection Systems.” URL: http://www.itsc.state.md.us/oldsite/info/internetsecurity/BestPractices/Intrusion.htm (12 August 2004).