Global Information Assurance Certification Paper

Douglas T. Rupinski

Submitted on June 9th 2004

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

Abstract / Summary

The following document is being submitted to fulfill the practical section for GIAC's Information Security Fundamentals (GISF) certification. The document addresses specific areas of the certification from the standpoint of a fictitious company called GIAC Enterprises.

Table of Contents

1. Description of GIAC Enterprises

GIAC Enterprises (The Company) is a 15 year-old software solution provider serving the Mid-Atlantic region. The Company provides full service software development, infrastructure architecture and application services. The main focus of business development in recent years has been within the Health Care industry.

The core revenue stream is derived from business relationships with companies in the Health Care industry. These services include EDI transaction Clearinghouse services as well as transaction translation implementation services. The Company's revenue last year was $62 million and forecasts reflect an increase in Clearinghouse services revenue of 55%.

The IT department supports internal services as well external services provided to customers. The main focus of the internal services is the Data Center. The Data Center provides Clearinghouse services to our customers and provides data confidentiality, integrity and availability. The IT staff also provides HIPAA implementation services such as Gap Analysis, custom EDI transaction translator solutions, and other non-Health Care related software services.

The Company has resources at 2 locations. The main office is located in Frederick, Maryland and runs the bulk of business services. The Texas office is used mainly as a "hot" site but also provides services to local customers such as hosting services, backup / recovery services and data vault services.

The Company has a total payroll of approximately $2.1M for a total staff 22 people. The position breakdown is as follows:

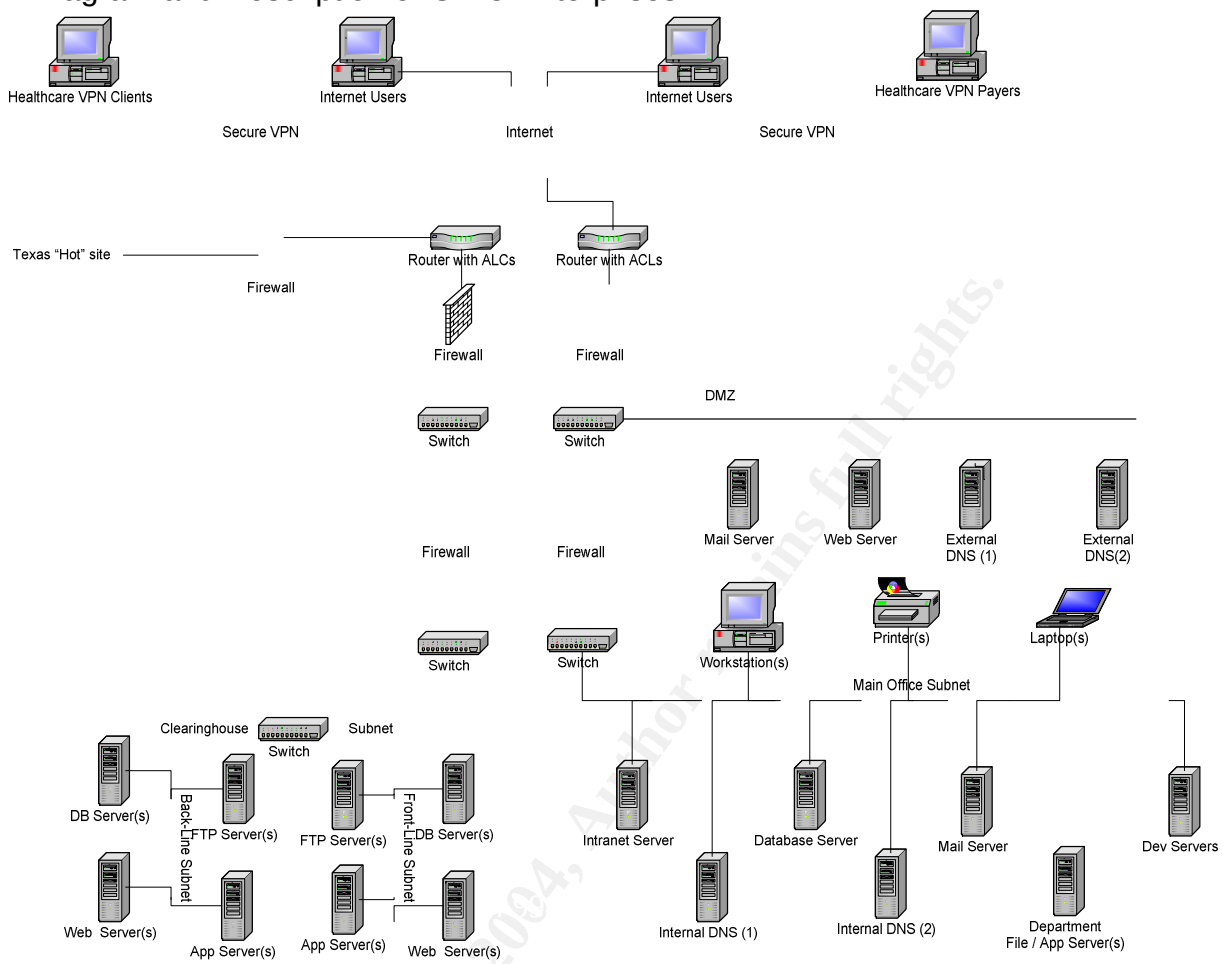
Main Office:

1. Senior Management
    a. President (CEO) – $300K
    b. Chief Financial Officer (CFO) - $225K
    c. Chief Technology Officer (CTO) - $160K
    d. VP of Sales - $125K
2. Administrative Staff – 3 totaling $90K
3. Sales Staff – 3 totaling $300K
4. IT Manager – 1 totaling $85K
    a. Network Staff
        i. Security Officer – 3 totaling $200K; avg. billable rate $175 /hr
        ii. Network Admin – 1 totaling $75K; avg. billable rate $125 /hr
        iii. Network Engineer – 2 totaling $150K; avg. billable rate $125 /hr
    b. App / Dev Staff
        i. Senior Developer – 3 totaling $225K; avg. billable rate $105 /hr
        ii. Junior Developer – 1 totaling $45K; avg. billable rate $75 /hr

Texas Office:

Network Engineer – 1 totaling $80K; avg. billable rate $125/hr

2. Diagram and Description of GIAC Enterprises



Because of the Clearinghouse services, The Company has implemented a high availability network. The network makes use of redundant devices such that failure of any 1 of the routers, firewalls or switches would still provide access to the Clearinghouse subnet. The border firewalls and routers are configured forward traffic to the DMZ and drop all other traffic not authorized for the internal network. If the traffic passes through the DMZ, the internal firewalls will drop all traffic not authorized for the internal traffic. At this point the switches will route the traffic as appropriate.

The network consists of a DMZ zone that allows for mail relay services between internal and external mail. The DMZ also provides a web services for the companies web site. On the internal side of the DMZ zone lays 3 screened subnets. The Main Office Subnet is designed to handle network traffic for office workers including internal mail services, name resolution with forwarding capabilities to the external DNS servers, file and application servers, and a development environment.

The Clearinghouse subnet is sub-divided into 2 screened subnets. The Front-Line subnet provides direct access to Clearinghouse services. The Back-Line subnet is implemented to provide a “Validated” Clearinghouse data repository.

3. Description of Office at GIAC Enterprises

Mission Statement

To provide the highest quality of services to our customers using currently accepted "best practices".

The IT Manager is responsible for 3 main areas and reports directly to the CTO. The first area of responsibility is to our existing customers. The IT staff is responsible for the smooth and un-interrupted network communications between our customer networks and our networks. The second area of responsibility are the services provided to offsite customers in areas such as network service implementations, security audits, backup and recovery services and network analysis. The last major area of responsibility is working with internal staff (Sales Staff, Application Developers, etc) to develop new business.

The IT Department affects the revenue stream in 2 different ways. The biggest impact on the revenue stream is through the smooth and reliable network infrastructure provided to customers for EDI transaction processing. The price model used by The Company for the Clearinghouse services is based upon the how much bandwidth customers use. The other revenue stream generated by the Network department is by providing our internal expertise to customer's offsite. This would include building networks from the ground-up, configuration of servers, security audits and the like.

The following items are under direct control of the Network Department:

1. Laptop and peripherals – issued to all Network Engineers; several "floaters" are available from a secure location at the office
2. Diagnostic hardware – retained within office and issued to Network Engineers when needed
3. Test Network – machines, switches, routers, firewalls, backup hardware
4. Documentation
    a. Acceptable use Policies
    b. Change Management Procedures
    c. Disaster Recovery Procedures
    d. Backup / Recovery Procedures

IT Manager - The IT Manager is responsible for supporting all aspects of IT such as the reliable operations of the Data Center, department servers, workstations, field equipment and telecommunications.

Network Engineers - This position is responsible for designing, engineering, configuring, installing, testing, and documenting system architectures and component configurations.

Developers - This position will be responsible for planning, designing, coding, testing, implementing, and maintenance of software applications.

HIPAA Privacy Officer - The expertise of this position is within IT Security but specifically with HIPAA privacy policies: administrative procedures, physical safeguards, technical security services and technical security mechanisms[1].

Security Officers - The expertise of this position is within IT Security and has the ability to provide customers with complete IT Security analysis.

The budgeted expenses for the IT Department are estimated to be $1.4M for the current fiscal year. Yearly budgets are develop by the IT Manager and CTO and are approved by the CEO. Below are the budget details:

1. IT Department salaries and benefits – $1,287K
2. IT staff equipment – $35K
3. IT Department (test networks only) equipment - $75K
4. IT staff software / licenses – $10K
5. IT Department (test networks only) software / licenses - $35K
6. IT Department training - $35K

The total company salaries are estimated at $2.1M (22 total staff members) with approximately half of this figure allocated to the IT Department (12 staff members). Without including monies from existing customer contracts, the IT Department generates an estimated net income of approximately $.9M. These numbers are based upon billable work rates of $120/hr for an average of 1,500 hours per year for all IT staff.

[1] "Especially for Clearinghouses". URL: http://www.ndedic.org/hipaa_clearinghouses.html. (5/20/2004)

4. Job Description at GIAC Enterprises

My official job title at The Company is “Security Officer I” and is a junior level position within the IT Department. The salary range for this junior level position starts at $40K and progresses to $65K. My salary is currently $55K per year and is based upon my previous work experience.

The documentation that I produce from my duties will be reviewed and critiqued by my co-workers. Summary evaluations will be provided to the IT Manager, my supervisor, and will be used as part of my yearly performance appraisal.

My primary responsibilities reflect activities that are related to customers and are as follows:

1. Analyze customer IT Security deficiencies
2. Perform and Document customer Risk Assessments
3. Review and/or Initiate customer Incident Response processes
4. Design / Develop Security Policy
5. Design and Implement Disaster Recovery Plans
6. Design and Implement Business Continuity Plans

My secondary responsibilities reflect activities that are related to our internal networks and are as follows:

1. Provide in-house Security Incident handling
2. Perform in-house Log Monitoring
3. Document Unwritten Policies
4. Research and Recommend Security Tools

5. How business is conducted at GIAC Enterprises

The core business focus of The Company is within the Health Care industry and more specifically with the Clearinghouse services provided to our customers. This service relies upon our Data Center to provide uninterrupted data flow to and from customers. The Data Center is the heart-beat of the company.

The following is a high-level flow for the Clearinghouse services:

1. Our customers create “non-standard” invoice data from their Accounting applications and then submit this data to us
2. We then process this “non-standard” invoice data to generate “standard” invoice data based upon HIPAA regulations.
3. This “standard” invoice data is then electronically transmitted to Payers (Medicaid, Blue Cross / Blue Shield, etc.)
4. Payers then process the “standard” invoice data and transmit back to us “standard” remittance data.
5. We then process this “standard” remittance data to generate “non-standard” remittance data.
6. This “non-standard” remittance data is then electronically transmitted to our customers
7. Our customers then update their Accounting system with this “non-standard” remittance data to complete the cycle.

Customers use their existing systems to send and receive “non-standard” data. The Company will first perform a complete GAP Analysis to determine any deficiencies in their current system. If any deficiencies exist, the existing systems will be modified to remediate the deficiencies.

From the Clearinghouse perspective, there are two other services that keep the business thriving. The first service is a GAP Analysis and is an App / Dev department service that provides Health Care customers with an analysis and remediation plan that will bring their existing systems in line with HIPAA regulations. The actual remediation work closes the loop on the GAP Analysis. The second service is the offsite implementation of the HIPAA regulations for our Healthcare customers.

6. Application and Access requirements for business operations

To carry out business operations pertaining to the Data Center, The Company has established a single connection type. This type provides Health Care customers with a client-to-site VPN connection to transmit and receive EDI data. This type of connection can either be a high-speed ISP connection or a dial-up ISP connection. All inbound and outbound connections to 3rd party vendors (Payers) utilize a secure client to site VPN connection.

All customers / organizations that access the Data Center are required to read and accept (by signing) a Data Center Acceptable Use Policy (AUP). Network traffic is monitored and reviewed on a regular basis for non-compliance of Data Center AUP. ACL's are applied such that VPN customers have only the necessary rights to get their job done.

The following pertains to all other business operations. All workstations are configured with a standard configuration such as Email, Internet connection, Office applications and Virus detection software. Workstations are also hardened based upon current "best practices". Additional software may be required to perform specific duties such as the IT Department. Each workstation is also configured to receive and automatically install critical patches / updates to Operating System software and Virus protection software updates. Each employee is assigned to a single workstation and is setup within the network with the proper ACL's that ensure that enough access is available but no more than needed to perform their duties. All employees are assigned a network user name and initial pass-code.

All employees are required to read and accept (by signing) an Employee AUP. Network traffic is monitored and reviewed on a regular basis for non-compliance of Employee AUP.

7. “Crown Jewels” (3)

The main “Crown Jewel” is the Data Center. Among the many services it provides, the main function is to provide Clearinghouse services to our Health Care customers. By having this service, The Company is provided with a substantial cash influx through health care EDI processing. The Data Center is considered a “Crown Jewel” because of the substantial investment that was required to get the existing Data Center EHNAC Accredited.

The second “Crown Jewel” is our many relationships with health care payers; the entity that provides payment to health care provides (our customers). With these relationships, the health care provider-to-health care payer loop can be connected using our Clearinghouse service.

The third “Crown Jewel” is our personnel. Not only was there a substantial investment in getting the Data Center EHNAC Accredited but there was a substantial commitment to hire, train and maintain a highly talented technical staff to handle all aspects of the Data Center, Network and Security services.

The Company uses a Customer Relationship Management (CRM) intranet application system to manage customer information as well as manage prospect information. The CRM application is installed in the internal Web Server and uses an authentication method to provide access to the following groups:

1. Senior Management – Provides direction and dictates what functionality is available to company staff.
2. Administrative Staff – Performs reporting for Senior and Sales staff, initial entry for new customers and prospects, and general maintenance for non-customer / prospect data (i.e. reason codes, status codes, etc.)
3. Sales Staff – Provides specific information as it pertains to any communications between The Company and the customer or prospect (i.e. prospect signing contract, emails, phone conversations, etc.). This group is further restricted to their own Customer / Prospect data.
4. Network Administrator - responsible for application availability, backup scheduling and application maintenance.

The Customer Relationship Management (CRM) intranet application provides the ability to generate pre-built and customized electronic contracts. Finalized electronic contracts are stored on the internal Web Server. This intranet application uses an authentication method to provide access to the following groups:

1. Senior Management – Have the ability to view all contracts
2. Sales Staff – Have the ability to view their customer contracts only
3. Administrative Staff – Have the ability to view general information on all contracts. This does not include details of the contract.

The Company uses a Back-Office Management (BOM) intranet application to manage personnel information such as Salary, Performance Reviews, Background Investigations, and Performance Awards. The BOM application is installed on an internal Web Server and uses an authentication method to provide access to the following groups:

1. Senior Management – Provides direction and dictates what functionality is available to company staff.
2. Administrative Staff – Performs reporting duties for Senior Staff, general data maintenance functionality
3. IT Manager – Performs duties that pertain directly to responsible staff
4. Network Administrator - responsible for application availability, backup scheduling and application maintenance.

Another “Crown Jewel” not mentioned would be the data in the CRM application. The CRM application provides an access point to a wealth of information about current customers, past customers, prospects, contacts, communications between customer and prospects, contract information, RFP documents, SOW contracts, purchasing contracts, leasing contracts, etc. This wealth of information if it fell into the wrong hands could prove detrimental to The Company.

All access to data to the above systems is strictly controlled using physical as well as electronic measures and is monitored for auditing purposes.

Physical control is implemented using a locked server and rack. Server and rack keys are held only by the CTO and IT Manager. Duplicate keys are held within the office fire-proof vault. The Data Center is made secure by use of a pass code lock. The pass code is issued only to the CTO and the Network staff. The building is made secure through the use of a pass code. Employees of The Company are issued unique pass codes.

Electronic control is implemented using Network, Router and File ACL’s. The servers are electronically secured using network user name and passwords. User name and passwords for the servers are written on a piece of paper and inserted into an envelope. The envelopes are secured in a lock-box that is placed within the office fire-proof vault. Keys for the lock-box are held by the CTO and IT Manager. The fire-proof vault entry code is held by Senior Management.

All access not explicitly identified above is strictly prohibited and is covered as part of the AUP.

8. Insider threat vectors for “Crown Jewels”

As much as The Company tries to reduce risks, there will always be some degree of risk within the company. Risk is the sum of vulnerabilities and threats. Reduce either one of these and risk will be reduced. Risk, Vulnerability, and Threat assessments are all used in an effort to reduce IT risks to the company. Threats represent possible danger to the company (either electronic or physical) and require a careful assessment to identify sources of danger and the level of danger each source represents. Not all threat sources can be identified, but one source is that of the insider. An insider is an employee of the company that has access to some or much of the internal workings of the company and has some motivation to do harm to the company.

The reasons used by an insider could include: proving that vulnerabilities do exist, feeling slighted from not getting a promotion or raise, personal vengeance against the IT staff for responding improperly to a complaint.

Proper use of risk reduction techniques such as Defense-in-Depth and Principle of Least Privilege can reduce this threat vector.

The CRM system provides access to customer and prospect information as well contract information and is a vital part of the business operation.

Access and Motivation

Printers are located throughout the offices and people can come and go as they please in these areas. Someone printed a copy of the yearly sales details of all Sales staff and left it at a printer until they could retrieve it in the morning. In the meantime, someone in the IT Department sees the report and notices the commission numbers for contracts that he/she worked on with the Sales person. Apparently it is very upsetting to the IT person because he/she did all the work and the Sales person received all of the commissions. The IT person immediately destroyed the Sales person’s data and left the company.

The BOM system provides access to internal personnel information and contains highly sensitive information.

Insider Access and Motivation

An IT person is unhappy with his/her latest performance review. The promotion and bonus that seemed to be in the works suddenly fell through. Word is that co-workers have provided some unflattering documentation to the IT Manager. This IT person needs to know what was documented and who did the documenting. This IT person sets up Snort to sniff the network for the proper user name and password that would allow access in the BOM system. Once in, she/he will be able to determine who and what was said. After this information is discovered, he/she will alter the data of the individual responsible for the poor performance review.

The Data Center “Crown Jewel” is the center of business. Digression in any of the security pillars represents a major failure which could lead to disruption in business operations. All possible measures are to be taken to ensure that Data Center services are available, have integrity and remains confidential.

Insider Access and Motivation

An IT person is unhappy with his/her latest performance review. The promotion and bonus that seemed to be in the works, suddenly feel through. Word is that the IT Manager has a personal issue with the IT person but will not reveal the issue. To get back at the IT Manager, the smooth and uninterrupted operations of the Data Center will need to cease; at least temporarily. The IT person will need the assistance (although unknowingly) of the CTO who can provide the required access. The IT person calls the CTO during a time when everyone else in the department has left and requests access to reconfigure the router due to a support call from the customer. Once access has been gained, the IT person will reconfigure the routers to drop certain inbound traffic. After a day or two, someone who was sending this traffic will realize that all is not well and the IT Manager will be in the hot seat just as planned.

9. Outsider threat vectors for “Crown Jewels”

The Data Center “Crown Jewel” is the center of our business. Digression in any of the security pillars (Confidentiality, Integrity, and Availability) by an outsider threat represents a major failure which could lead to disruption in business operations. All possible measures are to be taken to ensure that data flow through the Data Center is available, has integrity and is confidential.

There are many types of threats that can cause a disruption within the IT services. Threats can be physical or electronic. Physical threats include business operations located too close to flood or war zones. Electronic threats come in many forms such as Denial of Services attacks. Internal as well as external threats exists and the proper use of risk reduction techniques such as Defense-in-Depth and Principle of Least Privilege can help reduce these threats.

The reasons used by an outsider may include: proving that vulnerabilities do exist, to gain a competitive edge, and personal vengeance against the company for perceived business practices.

Denial of Services (DOS) is a threat that while not directly affecting data confidentiality or integrity, it does affect data availability. A skilled person may be able to replicate the client side of the client-to-site VPN connection. Once replicated, a carefully crafted packet could be sent down the tunnel to our Data Center. If the packet can get past the VPN Firewall and IDS, it can create any number of harmful outcomes. Prior to this occurring, this skilled person would have to do his/her homework to determine what vulnerabilities exist at either end of the VPN tunnel.

10[1]. Malicious code threat vector for “Crown Jewels”

The Data Center provides core business operating services. Any threat to these services should be reduced by all prudent means possible. Malicious code provides one possible threat to this service.

The W32.Welchia.K worm exploits Windows NT 4.0, 2000 and XP vulnerabilities in the ntdll.dll file. This worm may cause the operating system to fail or allows the attacker to execute code in the “LocalSystem” security context. The exploit is initiated when the hacker sends a specially formed HTTP request to the web server running IIS.

An operating system failure or the execution of unauthorized code is a threat that should reduced with all possible precaution and speed. The impact on The Company could be enormous; loss of revenue (servers being down), loss of data integrity, and ultimately, loss of reputation.

To exploit this vulnerability within the Data Center, either an internal attacker exists, a attacker has gained access to a VPN connection, or a router and/or firewall is mis-configured that would allow someone on the public network to send a HTTP request to a web server within the private network of the Data Center.

[1] Microsoft, “Microsoft Security Bulletin MS03-007”. 3/27/2003.
URL: http://www.microsoft.com/technet/security/bulletin/MS03-007.mspx (5/20/2004)

11. Identification of most severe threat

The Data Center is considered without a doubt the “Crown Jewel” of the company. It presents the largest investment within the company and provides the largest percent of operating revenue. Any threat to these services should be reduced by all prudent means possible. Denial of Services (DOS) attacks represents the “most severe” threat to the Data Center and can be initiated either by internal or external sources.

This type of threat is somewhat likely because of the: 1.) Services offered; 2.) Controls implemented; 3.) Control NOT implemented. The Data Center offers many services such as Web, Database, FTP, and Email. Each of these services offers DOS opportunities to a skillful person. Proper policies, software patch and service pack management procedures, and industry standard configurations can help keep known DOS threats from appearing. The controls implemented to control threats also offers DOS opportunities to a skillful person. These controls such as firewalls and routers also require proper patch management procedures and configurations. Controls not implemented include IDS systems both within the DMZ and the internal networks. This type of control would be able to provide egress filtering for attacks from an internal source.

Even with the implementation of policies, procedures and “best practices”, the Company still regards DOS threats as the most severe threat because of the damages that can occur. Without the smooth operation of the Data Center, Clearinghouse services can become non-operational. The DOS threat can also ruin the reputation and good name that The Company has established over the years. This type of threat could also include legal action if the implemented controls are proven not to be industry standard.

12. Remediation strategy for threat vector

The remediation strategy is to implement an IDS software package to provide the necessary controls to reduce DOS threats. The IT Department will need to provide an IDS recommendation (16 total hours) that will include budget for software, training (1 member of the network staff and 1 member of the security staff), implementation and maintenance. The initial budget for the IDS system implementation is $25,000; a yearly management budget of $2,500 is assumed. Once the recommendation has been approved by the IT Manager, the IT Department will proceed with the acquisition and training (32 total hours). The trained staff along with another IT staff member will then provide an IDS Implementation & Monitoring plan (24 total hours) to the IT Manager. Once this is approved, the plan is executed (80 total hours). The IDS machines are hardened and stripped-down to include only needed services to run the IDS software. The total time required to implement the IDS system is approximately 160 hours.

The total implementation cost for the network IDS system is $24,600 and is detailed below:

Software

1. Snort – freeware

Hardware

1. Medium Range IDS machines – $18,000 (4 @ $4,500 each; estimated)

Training[1]

1. Classes – $6,600 (2 @ $3,300 each person per phone quote)
    a. Building and Operating Snort – 2 days
    b. Snort Rules – 2 days

This type of implementation will protect the networks by detecting attacks, stopping the attack, checking firewalls, verifying security polices, documenting attacks, and catching insider hacking among other benefits[2]. As IT staff becomes more familiar with network traffic being allowed, IDS filters/rules can be reviewed and implemented.

[1] "Sourcefire Training Services". URL: http://www.sourcefire.com/services/training.html
[2] Bryant, Mitch. "The integrated partner for your firewall". 4/23/03.
URL: http://techrepublic.com.com/5100-6313-5029665.html

13. Backup strategy reviewed

An enterprise-wide assessment has determined that not all business related data is being backed-up. While most employees store business data on the appropriate file servers, there are some employees that have not accepted this as part of their responsibility. To mitigate the damages that may result by workstation data unavailability, an enterprise assessment was performed to determine the most cost-effective measure to ensure that all workstation data is backed-up (Supplemental Backup).

The approach favored for the Supplemental Backup is to use department servers as backup devices for the workstation data and then have the enterprise backup process include the Supplemental Backup data along with the normal department server data. The reason for this approach is to ensure that all data is backed-up, reduce or eliminate the need of users to be responsible for performing backups, labeling tapes, inserting new tapes, etc. This plan also takes advantage of the existing enterprise backup process and the ample available disk space on the department servers.

After reviewing the network environment, number of workstations (25), and size of workstation disks (30 GB average), the following requirements was identified:

1. Must be a centralized backup solution
2. Must have an Administrative web console
3. Must require minimal (at worst) workstation user intervention
4. Must minimize the amount of data traveling over the network
5. Must have ability to backup database files

After reviewing specifications on several software packages, Veritas Desktop and Laptop option was selected for 2 major reasons. This application met the software requirements and it was cost effective because it leveraged the existing enterprise backup system.

The selected software will be installed on the server that Veritas Backup Exec is currently installed on. Then each workstation will be remotely installed and scheduled for regular backups. It was suggested that this Supplemental Backup was to be performed monthly. However, it is recommended that departments break-up the Supplemental Backup so that some are performing the backup on week 1 while the remaining backups are performed on week 2.

The Supplemental Backup data will be protected as follows:

1. ACL's are implemented that allow owners and Network administrator's access or restore rights to the data.
2. Auditing is setup for the data files and is included as part of the enterprise-wide monitoring process.
3. Department servers are located within a secure room

4. Access to the secure room is by pass code.

Costs:

A. Software Product(s) - $326

Veritas Desktop and Laptop Option - $326 for 100 workstations

B. Hardware

Hard Drives – No additional hardware is required
Media Tapes – No additional media is required

C. Implementation Costs – 40 hours X $125/hour (normal billable rate) = $5,000

1. Initial Workstation Backup Implementation – 20 hours
    a. Desktop and Laptop Option installation on Backup Exec media server
    b. Desktop and Laptop Agent configuration

2. Workstation User – this requires no user intervention

3. Ongoing Workstation Backup Maintenance – estimated at 20 hours

    a. Software upgrades
    b. Workstation configuration tweaks

14. Offsite backup strategy reviewed

The current enterprise backup process includes backing-up all production servers and verifying backups by scheduled restores. The backup tapes are then placed within the main office fire safe. Part of the process that is missing is to provide a safe and secure location for the backup tapes. Up to this point, an off-site storage location has not been implemented but circumstances now require that tapes become available in case of an enterprise-wide disaster. If such a disaster does occur, the off-site storage facility would be able to provide the latest copy of the enterprise data.

The approach that The Company will adopt is a three-layer approach that includes off-site storage as well as a modification to the on-site storage process. The off-site layer includes a 3rd party service that will securely and safely store the backup tapes. To increase data availability in case of disaster, the Texas office will be provided with nightly tape backups as well. A third copy of the backup tapes will be retained within the main office fire safe as before.

The following features should be provided when selecting a 3rd party service[1]:

1. Safety
2. Fire Protection
3. Flood Protection
4. Environmental Control
5. 24-hour access

The tapes at either the 3rd party service or the Texas office will be stored within a small locked box which is locked within a climate controlled room. For the tapes stored at the main office, the tapes are stored within a small locked box which is locked within a fire safe. The backup software encrypts the data for confidentiality and then the backups are hashed to provide integrity. The 3rd party service provides 24x7x365 data availability and a 2 hour delivery window. The tapes at the Texas office also provide 24x7x365 data availability but the delivery window varies.

There are a couple of one-time tasks needed to begin the off-site storage of backups. They include: selecting a company that provides the service, providing a budget for the service and the ancillary items (i.e. additional media tapes), assigning responsibility to internal staff to manage the process (i.e. daily pickup of tape), updating Disaster Recovery and Business Continuity Plans to reflect new processes and creating a Restore Test Plan.

[1] Thornberry, Suzanne. "Vaulting is best practice for data backup plan". 9/24/2002 URL: http://techrepublic.com.com/5100-6298-1059546.html (5/20/2004)

The following tasks will need to be repeated:

1. Backups are provided to service for off-site storage - Daily
2. Restore Test Plan is executed – Monthly
3. Tape life-span / number of stores will need to be managed

The Restore Test Plan will need to be created by the IT Department and will provide the necessary audits to insure that the backup and restore processes are accurate and reliable.

15.[1] Business Continuity Plan – Guerilla style

The high-level approach that addresses guerilla Business Continuity Plan (BPC) is to restore the Health Care business services as quickly as possible. The approach will address the "one-percent" philosophy and represents an initial look at recovering business services. As time and resources become available, this plan will be expanded to include all business process.

A disruption within the Health Care business services would prevent customers from sending health care invoices to payers and payers from sending remittances to our customers. This represents a substantial risk to The Company. This disruption needs to be quickly addressed and remedied as quickly as possible to reduce downtime for customers and payers.

In the event of a disruption, the following events will occur:

1. Network administrators should be contacted (phone or beeper) immediately by system processes.
2. Network administrators should contact Senior Management by phone and email.
3. Senior Management and network administrators determine the level of disruption, the effected systems, and the estimated disruption duration.
4. Senior Management communicates to "hot" site to begin with "Go Live" plans
5. Senior Management designates home office as "fully" or "partially" abandoned. If "partially", the extent will be detailed.
6. Administrative staff will then be notified to initiate communications by phone and email (during off hours) or internal communications (during office hours) to Department Managers as to the current status.
7. Department Managers will communicate this information to their staff by phone and email (during non-business hours) or internal communications (during business hours).
8. Senior Management and Sales staff will then begin the process of communicating by phone with customers and 3rd party vendors.
9. Recovery Team is relocated to "hot" site
10. Recovery Team assists with "Go Live" plans at "hot" site
11. "Hot" site is declared "Live"
12. Begin recovery of disrupted site or search for new site.
13. Recovery Plan terminated when all services are fully functional.

Senior Management is the only group authorized to initiate the recovery plan. They are also the only group authorized to communicate with the press or public. Contact lists are inserted into paycheck envelopes and are also available at the BCP secure web site.

To fully validate the BCP, The Company would be required to simulate a full disruption. While this would certainly validate the plan, it may bring about unwanted stress by/from our customers and 3rd party vendors. Therefore, to validate and correct inaccuracies

[1] SANS. "Policy, Procedure, and Strategy". File: SECPLUS_65_0403.pdf

within the BCP, Senior Management will designate “simulated” disruptions during the course of the year. These simulated disruptions will designate various levels of disruption and indicate the steps of the BCP to be completed. While this in no way fully validates the BCP, it should provide a somewhat accurate sense of the completeness of the BCP. Upon completion of every “simulated” disruption, Senior Management and IT Staff will review results and make recommendations to be incorporated within the BCP.

“Go Live” Plans

1. Verify that previous day’s home office backup is restored
2. Prepare for “Go Live” Test Plans
3. Restore any current days home office backup
4. Execute “Go Live” Test Plans
5. Verify test results

Recovery Team:

1. Senior Staff member - 1
2. Administrative Staff – 2
3. Sales Staff – 0
4. Network Staff
    a. Network Manager - 1
    b. Security Officer – 1
    c. Network Engineer – 2
5. App / Dev Staff
    a. App / Dev Manager - 1
    b. Senior Developer – 1
    c. Junior Developer - 1

”Hot Site”

1. The Company BCP secure web site
    a. Includes BCP plan
    b. Contact List – cell phone, beeper, email and role
    c. Recovery status – level and affected systems
2. Replicated network infrastructure of main office NOC
3. Previous day backups of main office NOC
4. Offices adequate for Recovery Team
5. Office supplies

16. References:

1. Microsoft, “Microsoft Security Bulletin MS03-007”. 3/27/2003. URL: http://www.microsoft.com/technet/security/bulletin/MS03-007.mspx (5/20/2004)
2. Veritas, Data Protection and Synchronization for Desktop and Laptop Users , URL: http://www.veritas.com/Products/www?c=option&refId=143&productId=57[i]
3. **“**Sourcefire Training Services”. URL: http://www.sourcefire.com/services/training.html (5/27/2004)
4. Bryant, Mitch. “The integrated partner for your firewall”. 4/23/03. URL: http://techrepublic.com.com/5100-6313-5029665.html (5/27/2004)
5. “Especially for Clearinghouses”. URL: http://www.ndedic.org/hipaa_clearinghouses.html. (5/20/2004)
6. Thornberry, Suzanne. Vaulting is best practice for data backup plan”. 9/24/2002 URL: http://techrepublic.com.com/5100-6298-1059546.html (5/20/2004)
7. SANS. “Policy, Procedure, and Strategy”. File: SECPLUS_65_0403.pdf