GIAC Enterprises: Security Policies for a Non-Profit Organization

Introduction to Information Security SANS Online Training Track 9 (GISF)

Practical Assignment
Linda G. Redding
Submitted November 23, 2004

Table of Contents

Abstract

The following document was prepared to fulfill the requirements of the practical assignment associated with the SANS Self Study Track 9: Intro to Information Security (GISF) Certification.

The document will demonstrate the author has acquired knowledge of the basic terminology and concepts of information security.

1. Description of GIAC Enterprises

GIAC Enterprises – A Non-Profit Organization (GENPO) is an organization with the mission of encouraging, educating and reaching out to individuals to promote their religious faith and spiritual maturity.

Because GENPO is a non-profit organization, we rely on donations from individuals, locally and beyond. It is a requirement that GENPO be good stewards of these funds, to this end the entire staff is dedicated to viewing the financial aspects of this organization from a business standpoint. We continually protect the personal and confidential information of our supporters and customers as well as handling these funds in a responsible manner.

GENPO's net income is an average of $1.58M each year. The IT/IS department plays a key role in earning this revenue as they clearly demonstrate the ability to maintain the confidential information of each supporter. In addition, we are committed to expanding our knowledge to enable us to communicate effectively with the ever-changing technical environment in the world today.

With our main campus located in Brandon, Florida, we have successfully secured six buildings, identified as: the main sanctuary; the main office; three educational buildings (which includes an extensive media center and first class Daycare facility with 7 classrooms); and the family life center (which includes a social/dining hall and gymnasium).

Our organization has a payroll of $711K for a total 18 full-time employees and 17 part-time employees. The breakdown for the staff is as follows:

Senior Pastor	$60K
Counseling/Administration	$52K
Music Ministry	$46K
Music Associate (part-time)	$6K
High School Student Ministry	$44K
Middle School Student Ministry	$42K
Senior Adult Ministry	$38K
Children and Family Ministries	$44K
Young/Median Adults & New Members	$48K
Women's' Ministries(part-time)	$11K
Media Ministries (part-time)	$10K
Support Staff (5 admin assistants)	$90K
Accounting Manager	$40K
IS/IT Department (4 on staff)	$140K
Daycare Personnel (14 part-time)	$40K

2. Diagram and Description of GIAC Enterprises

An internal user desiring to access the internet must pass through the Proxy Server. We have set the firewall rules to allow the proxy to pass. The proxy contains filters blocking access to inappropriate sites as well as providing logging of all activity.

The workstations all have RFC-1918 addresses, which do not allow them access to the internet without a proxy server. The 3 workstations pictured in figure 1 represent the 25 workstations we currently host on the LAN. The proxy server has ACLs (access control lists) that allow only internal addresses to access it.

Should the users desire to reach their e-mail, the connection would utilize a POP3[1] connection through the firewall, then on to the e-mail server. Incoming e-mail would have come in via the internet and would have passed through any 'blocked content' rules that have been applied by the administrator. The mail server will reject e-mails that do not pass the rule sets.

External users who want to access the GENPO application systems will pass through the primary firewall to the 'content free' Web Server, utilizing port 80, with the exception of port 25 for mail, and port 443 for SSL. The purpose of this server is to serve as a proxy to the systems behind, thus preventing any direct connections from the public internet. All other ports are blocked by the firewall. Accounts for users are created upon submission of an appropriate account request form. Upon successful verification of individual identifying information, an access account will be created.

When a user initially connects to the server the session is initiated as a conventional HTTP session, when they select login from the menu the session changes to an HTTPS session which is the mode in which it remains until they logout. The user access attempt will query to the LDAP server, which houses the previously created user accounts. This query will return a status indicating successful or unsuccessful log on to the application, at which time the user will be allowed to access those applications to which they are authorized. This will allow the potential customer/member to enter through the firewall to the Internal Web Server. This set up is ideal for the parents of the children in our daycare facility to access their child's personal information along with paying their tuition payments in a secure on-line environment.

The IT/IS department, along with the pastoral staff and other select staff members has direct access to confidential information utilizing VPN (virtual private network) connections. The communications inside the VPN tunnel are shielded from sniffing and eavesdropping. Since a VPN does not protect us from malicious traffic once it has entered the tunnel, we have added an IDS (intrusion detection system) to detect possible malicious conduct.

[1] "Webopedia", URL: http://www.webopedia.com/TERM/P/POP2.html, 21 Nov. 2004

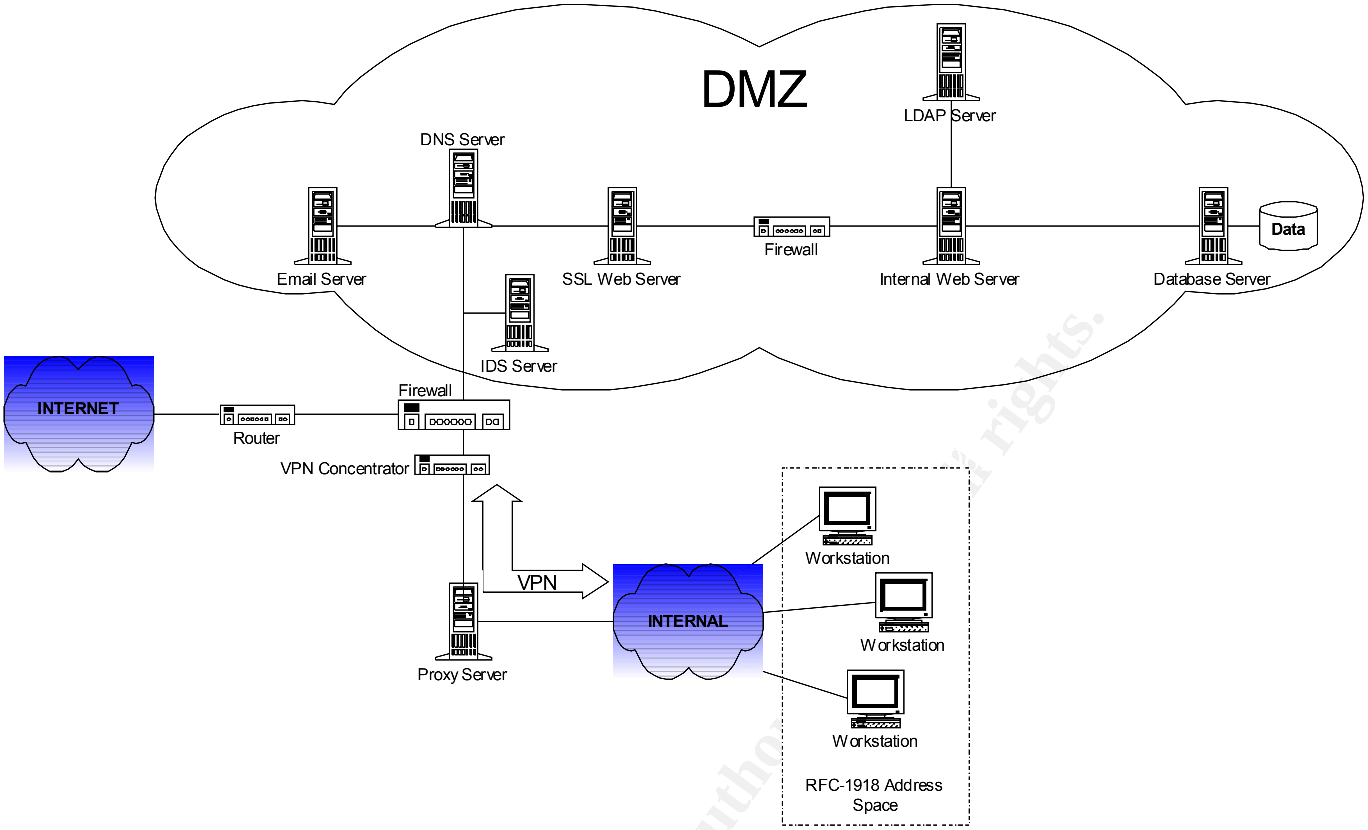
DMZ
LDAP Server
DNS Server
Email Server
SSL Web Server
Firewall
Internal Web Server
Database Server
Data
IDS Server
INTERNET
Router
Firewall
VPN Concentrator
VPN
INTERNAL
Proxy Server
Workstation
Workstation
Workstation
RFC-1918 Address Space

Figure 1

3. Description of my office at GENPO

The Information Security/Information Technology (IS/IT) department has a wide range of responsibilities, focused in four internal functions. These functions are:

- Security Operations – ID and password administration; firewall management; intrusion detection and system log monitoring and analysis
- Security Awareness and Education – training and promotional campaigns
- Incident Management – emergency response and incident investigation
- Technology Services – technology evaluation; implementation; operational support and research and development

Our mission statement was derived from the three pillars of Information Security; "Assuring integrity, confidentiality and availability to all". Our office supports GENPO staff, our member and customer base and financial contributors.

Because GENPO is a non-profit organization, a key primary objective is to proactively protect the current infrastructure, preventing loss resulting from viruses, worms, hackers and/or malicious acts. The IS/IT Manager reports directly to the Counseling and Administration Pastor. The IS/IT Manager and 3 IS/IT staff provide protection and support to the 18 full time and 17 part-time employees. Therefore, 14.55% of the staff is dedicated to the Security Department.

The expected budget needs for the GENPO Information Security Group has been set to $186K for the fiscal year, which is 8.86% of the expected annual earnings of GENPO. Of this, $186K, $140K is designated for salaries, with approximately $46K designated for departmental and staff equipment and software/licenses.

Confidentiality of financial records, including donations received and dispensed, along with daycare tuition records is a critical function of our department. The solid reputation GENPO has earned in maintaining this confidentiality has contributed greatly to the revenue of our Company. In addition, because the pastoral staff provides extensive counseling services to those in need, it is imperative these records be closely guarded and protected externally and internally. GENPO practices the Principal of Least Privilege by granting access to systems and networks only to those individuals who have specific reason for this access.

Each IS/IT staff member has been issued a laptop to enable them to provide 24x7 support. We are dedicated to ensuring our staff members can access the necessary resources needed, without interruption, and with complete confidence.

4. My Job Description at GENPO Enterprises

- Job Title: Security Operations Associate
- Salary level: $28,000/yr
- I am in the Security Operations Office and directly report to the Manager – Information Security/Information Technology
- My primary function as the administrator for account and password management. In this role, I receive access requests for our various online systems and ensure that the required system accesses are properly defined and that the initial, pre-expired passwords are distributed back to the requestor in a confidential manner. My measure for performance in this area is set by management and states that "no less than 98% of all access requests will be accurately completed within 24 hours of receiving each request."
- My secondary function is to coordinate the Security Awareness and Education area. My success measure is that 100% of all new staff must receive security orientation training and that new awareness materials (posters, mailers, etc.) must be developed quarterly.

GENPO Enterprises was impressed with the GIAC GISF certification I have earned and hired me as a full time employee one week ago. The manager has given me the assignment of documenting some of the company processes, completing a high-level risk assessment and contributing to GENPO's continuity plan.

To achieve this assignment, I will observe the current processes with "fresh eyes" looking for improvement opportunities others may have missed. This effort will shorten the training time I will need, as I will be completing an overview of GENPO's current structure.

5. How GENPO conduct its business

The end-to-end business flow of GENPO is primarily e-commerce based. Elements include:

- Public Website
- Secure Web Portal
- E-Commerce System (using SSL)
- Daycare Tracking System (DTS)

Other supplemental systems include:

- E-mail server
- Financial systems server
- Materials management server
- Media center server

Key business operational goals are to enable parents with children in our daycare facility to pay their tuition online in a confidential and secure environment and to remotely (via the internet) manage child profile information.

Profile Updates In addition, the DTS has profile records for each child, which includes: photographs, fingerprints, medication instructions, special dietary needs, emergency contact information, etc. This system is available to authorized daycare staff. Parents are given access to their children's records only. Access is controlled by unique account identifiers and associated strong passwords, which are generated by the system and assigned to each account at inception. Users may request password changes via a dedicated option in the system, at which time the system will generate another 8-character password using a random grouping of upper and lower case alphabetic characters and interspersing these with numbers and special characters.

Parents are permitted to update information for their children in the following areas:

- Emergency contact information
- Current medicine(s), dosages, etc.
- Allergies and special dietary needs

Authorized staff members may update:

- Fingerprint records
- Photographs of the children
- Daily child campus check-in/check-out records

Tuition Payments The DTS also provides for online tuition payments to be made via the web interface. Because of the sensitive nature of this information (i.e.-credit card numbers) an SSL interface is required. Access to this function is controlled via a challenge/response interface that requires a unique account identifier and a strong password. Payee profiles contain payment histories and profile information. Realtime updates regarding successfully cleared payments are mirrored to the financial systems SQL database.

6. Applications and types of access required

Customers, business partners, and suppliers connect to the various systems necessary for completing their specific tasks via a web portal application hosted on the SSL Web Server.

Suppliers for the various bulk supplies required by the daycare access the materials management server to check current inventory levels and make recommendations regarding supply purchases via e-mail to the Children and Families Administrator. GENPO processes these transactions via an SSL connection on the web servers.

Parents access the Daycare Tracking System via a web-enabled interface. After transiting a primary edge router, and negotiating the primary firewall, users access the public website server residing in the GENPO DMZ. This server acts as the presentation layer for the DTS system. Users are authenticated to the system via backend interaction with our LDAP server. All backend functions (database operations, LDAP transactions, etc.) are separated from the primary webserver by a secondary firewall, which allows only connections from the front-end server or administrative connections from the internal addresses or VPN.

Staff members are authenticated to the DTS system using the same LDAP server. Access to the public website server comes from the internal (RFC-1918 address space) network via the internal proxy server, through the primary firewall. Remote access by the staff is required for technical operations and support functions for the various components comprising the critical business functions. Access is made using a Cisco 3.5[2] VPN client.

[2] "Release Notes for Cisco VPN Client for Windows, Release 3.5.4" , URL: http://cisco.com/en/US/products/sw/secursw/ps2308/prod_release_note09186a0080104e35.html

7. The “crown jewels”

Our main “Crown Jewel” is our DTS (Daycare Tracking System) application. This application enables our staff and the parents of the children in our daycare center to access and update the child’s profile. This system is regarded as the differentiator between ourselves and other similar childcare facilities. Via the use of this system, parents enjoy a level of assurance regarding the well being of their children. Parents are especially appreciative of the staff’s ability to monitor campus entry and exit of each child on a daily basis. This systems database contains a considerable amount of extremely private and sensitive personal and financial information and so, as the main “crown jewel”, this system and it’s associated information must be protected.

Our second “Crown Jewel” is the secure web portal. Roles and privileges are established via use of the LDAP server. Depending upon the role that is associated with a given account identifier records may either be updated or viewed only.

- Parents have the ability to update and view only their own child’s records
- Daycare Staff members have view only access to all information. They also have update capability under the check-in/check out function
- System Administrators have the ability to view and update all information

All accesses are secured and profiles provide access to only the systems you are authorized to access.

Our third “Crown Jewel” is our financial systems comprised of our general ledger, accounts payable and materials management systems. These systems are responsible for enabling day-to-day logistical operations as well as supporting the financial life of the organization.

A fourth “Crown Jewel” that is not listed above is our personnel. The individuals associated with our organization are dedicated to supporting and adhering to the security policies defined by the IT/IS department. This would include observing the three pillars of information security; confidentiality, integrity and availability. Each employee understands and supports the need to protect our resources and reputation.

Customer and contact lists, contracts, which commit our office to purchase goods and services, and management information such as salaries, performance evaluations, background investigations and awards, are stored on a backend database.

Each user must log in with their specific login ID and password. The System Administrator applies permissions to each ID enabling them to gain access to the required area. User IDs are assigned roles, which determine the functionality and privileges they have within that area (read/write delete).

Currently, the following roles have been defined: View, User, Administrator and Security. The View role allows users view only access to those areas to which they are authorized. The User role has the ability to view and update their individual records. Users do not have the ability to delete records. The Administrator role and Security role has the ability to view update and delete all records. Among their other roles, the Administrator and Security roles provide oversight of other user activity, which protect against unauthorized or unapproved activity.

The development of the information housed on the backend database is as follows:

- Vendor contracts – Accounting Manger and her Administrative Assistant
- DTS customer and contact lists – Children and Family Minister and her Administrative Assistant
- Management Information – Counseling/Administration Minister and his Administrative Assistant

All of the above is maintained by the IT/IS Department who observes preventative strategies including separation of duties, helping to prevent fraud by separating tasks among multiple individuals and rotation of duties to help detect fraud by rotating individuals among tasks.

8. Insider threat vectors

As much as GENPO strives to provide complete protection against threats and vulnerabilities, we realize that good security is a continuous process consisting of analysis, prevention, detection and response.

Our crown jewels have been identified as DTS, secure web portal, GENPO financial information and our personnel.

DTS – our daycare tracking system contains information about each child associated with our daycare facility. The parents have the ability to update their child's profile and pay their child's tuition on a monthly basis.

Each GENPO employee is required to go through a personnel-screening process, which includes an extensive background check including criminal/credit history and identity checks. Our goal is to eliminate the risk a GENPO employee, especially one of our daycare workers, to have contact with our daycare children. With this practice, we hope to eliminate the possibility of a child offender's association with our organization.

Secure web portal – the secure web portal is the method used to access information stored on the database server. Roles are assigned to user ID's to give appropriate access to each individual. Internal users may have a desire to use this portal inappropriately to gain access to confidential information that is not meant for their access. The may attempt to do this by exploiting documented vulnerabilities in either the web or database server software. For this reason the systems and applications are patched as necessary. IT/IS must apply the patches to all systems. Additionally an IDS (intrusion detection system) is employed to monitor activity and notify IS of any unusual or malicious activity.

All of the salary information for each GENPO employee is housed in the financial database. An internal person may attempt to attain access to this secure area by acquiring the login and password of an Administrator. They may have a desire to compare their personal salary with the salary of another. They may attempt to do this by use of a network sniffer. It is for this reason that SSL is used when connecting to the web server.

The personnel at GENPO are encouraged and expected to adhere to all security policies defined by the IT/IS Department. Among those policies is the acceptable use of company resources. These resources would include internet use, telephone, copiers, faxes, and supplies. Should an employee have a desire to use the internet to access an inappropriate, this considered grounds for discipline and possible separation.

9. Outsider threat vectors

The GENPO DTS application is the 'Crown Jewel' that sets our daycare facility apart from our competitors. This online application could be destroyed, modified or copied if continual monitoring and protection are not in place.

A person may attempt to gain unauthorized because they have a desire to gain confidential credit card information belonging to the parents of our daycare children.

One technique an attacker could use to compromise the DTS application would be the use of various types of password attacks. A few of the common password attacks are known as:

- Personality profiling – attackers attempt to guess the user's password by reviewing the user's hobbies, names of family members, favorite sport teams, etc.
- Brute force attacks – attackers attempt to guess passwords by trying all possible combinations of available characters. These types of attacks are more difficult if the password uses special characters (!, @, &, %, #).
- Dictionary attacks – attackers work by trying each word in the dictionary as a possible password.

10. Malicious code threat vector

GENPO's financial systems is a key 'Crown Jewel' that contains highly sensitive and confidential information such as our general ledger, accounts payable and materials management systems.

The Trojan horse program is a type of malware that disguises itself as an ordinary, harmless program. Many times, the program enters a network via an e-mail attachment that an unsuspecting user believes is a useful download. When the user clicks on this attachment, it begins executing a program that can cause activities such as erasing files and directories, collecting passwords and sending sensitive personal information to other users. A Trojan horse can also be used to create a user account on your system and backdoor programs. Backdoor.Selka is an example of a Trojan program that allows a remote attacker to obtain unauthorized access to an infected computer[3]. These can create holes that allow access at a later time. This would enable access to sensitive areas by using the authorized user's password.

In the event of a compromise, the confidentiality of personal information could leave individuals vulnerable to identify theft, unauthorized orders and purchases. In addition, the outstanding reputation we currently have could be marred which would be difficult to recover.

11. Our most severe threat

The most severe threat the IT/IS Department currently strives to avoid is a lack of availability of our systems – disruption of service.

Much of our day-to day internal operations depend on gaining access and referring to the data in our applications. The success of the DTS application relies heavily on availability as we utilize this system to monitor the number of children for which the daycare facility is currently responsible.

At the beginning of each day, each child is checked into the system, remaining until the time he or she is checked out. Therefore, at any given moment, authorized users may query the system to determine how many children they are currently responsible for and who they are. In addition, emergency contact numbers are readily available at the touch of a button should there be a need to make such contact.

This threat could be a likely occurrence if protective measures are not continually implemented to prevent such an event. Viruses, worms, and network attacks are types of electronic threats that could have a negative effect.

[3] Symantec Expanded Threat List, 12 November 2004. URL: http://www.symantec.com/avcenter/expanded_threats/virus_worm_trojan_horse.html

In addition, because our campus is located in the central Florida area, the likelihood of physical threats, such as hurricanes and/or tornados, should be considered.

The potential losses resulting from the lack of system availability range from an inability to have an accurate record of daycare children check in and check outs, access to financial records, and the inability to accept or acknowledge tuition payments.

12. Recommended remediation strategy

The IT/IS Manager has been impressed with the observations and selections I have made and has requested that I prepare recommendations for remediation. The Manager has approving authority for IT assets and expenditures within our office up to a limit of $25,000.

Description of remediation strategy – In keeping with the goal of maintaining availability of our systems with little or no down time, I recommend we adopt the following measures to address each identified area of concern:

- **Misuse of resources by our users** (awareness campaign, monitoring)

    1. Develop Awareness Campaign: Estimated time frame - 3 weeks, Cost: $100, Resources:GIAC Certified IT specialist (myself), media specialist who has a Bachelor of Arts in Graphic Arts (Campaign to address: password strength and management, proper electronic communication techniques, “business use only” standard for usage)
    2. Institute Internet Usage monitoring: Duration: 2 weeks, Cost: $3200 (PC and Cyfin™ Reporting Software, ensure logging active on Squid Proxy)

- **Workstation security** - password protected screen savers

    3. Obtain required screensavers and mandate use. Duration: 1 week, Cost: $0, Resources: IT generalist with basic PC skills to setup screensavers

- **Physical security** – securing all sensitive and confidential information under lock and key (publish policy document)

    4. Mandate use of existing locking cabinets and fireproof safes, highlight usage requirements during awareness campaign. No duration, no cost, no resources required.

- **Network security** – IDS platform.

  5. Implement IDS, Duration: 2 weeks, Cost: $1400, Resources: Experienced intrusion detection analyst (currently on staff) (Purchase 1U server, download/install/configure OpenBSD operating system, download/configure Snort)

- **Proper disposal of sensitive and/or confidential information** – use of the shredder is mandatory

  6. Obtain 5 shredder deposit boxes and publish policy document, Duration: 1 week, Cost: $1500, Resources: None. (Highlight requirement for use of shredder boxes and shredder itself in awareness campaign. Stress importance of proper disposal of sensitive information[4].)

Total cost of recommended measures: $6200.00

13. GENPO's backup strategy

My Manager has advised me that although GENPO does have a current backup plan for the networked drives, there is no backup plan in place for the local drives. In addition, the current plan has not been consistently enforced. He recognizes this is leaving us in a vulnerable position and has requested that I develop a plan that would backup all of the data in our office. We are keenly aware that although we have shared network drives set up for critical data, there are individuals that continue to store important information on their local drives in violation of established policy.

High Level Approach

My manager has requested that backups be completed once per month. Realizing our goal of reliably saving critical data 100% of the time, I am recommending that backups be done in the following fashion:

- On the first Saturday night of each month a full image backup of the system(s) is taken.
- Every Saturday night (with the exception of the first one) a backup of the system is made which includes everything that has changed in the previous week.
- Every night (with the exception of Saturday) a backup of everything that has changed since the previous day is made.

[4] Datz, Todd. "Trash Talk." CSO THE RESOURCE FOR SECURITY EXECUTIVES. Volume 3 Number 11 (2004): Pages 60 – 62.

Backups will be stored on a department server. The software/hardware suggestions below will enable the backup administrator to quickly and easily select and restore desired data. Most of these tools are suggested because they are already on-site and are adequate for our desired goal.

Software/hardware needed and their associated cost for server backups

The server backups will be made using standard Unix utilities.

Tar (tape archive)	cost = 0
Rcp (remote copy)	cost = 0
DAT tape drive	cost = 0 (existing)

Software/hardware needed and their associated cost for workstation backups

The workstation backups will be made using standard Windows utilities.

Iomega 255 GB USB external hard drive.	cost = 12@$379.99 each
Windows NT backup software (already on the OS)	cost = 0

How these supplemental backups will be protected

All backups may be stored on a department backup server that will be housed in a secure room accessible by authorized personnel using a Cipher-lock. The backup server will have the external hard drive connected to it and all workstations will backup to it nightly. This drive will be rotated off site monthly and a new drive connected. It is anticipated that the workstation backup volume will be low owing to the fact that policy dictates that sensitive or business critical information is not to be stored on workstations.

Costs, including employee time to implement this solution for the first year

Implementation costs will be 40 hours x $50.00/hourly labor rate = $2,000
Costs of hardware/software = $4559.88
Total for first year = $6559.88

14. Review offsite backups

My manager is very happy that we have a recommendation in place for on-site backups. However, because these backups are stored at our facility, the backups could be destroyed or damaged in the event of a disaster such as a fire or hurricane. The following is a recommended approach to implementing an off-site backup process.

High level approach

All backups should be stored at an offsite location to prevent their destruction. With our campus located in Brandon, Florida, I suggest a facility located in Jacksonville, Florida which is some 200 miles from our location. In the event it is necessary to restore the system or specific files, these backups will be retrieved from the storage facility.

One time tasks needed to start this process

- Enter into a contract with a Jacksonville, Florida storage facility
- Implement the methodology of the backups
- Designate back up personnel

Repeating tasks

- Loading tapes
- Performing backups
- Rotating tapes – Tapes will be gathered for pick up and old tapes will arrive every Monday, based on an annual rotation
- Rotating the workstation backup media monthly.
- Paying monthly rental bill

Confidentiality safeguards to protect your data

All backup data should be considered confidential and not be viewed by unauthorized personnel. Only authorized personnel may perform backups and transport data. Because the backup media is sent offsite in a sealed and locked container, it is a simple matter to determine if the container has been breached. Additionally legal remedies are built into the contract if the vendors security is compromised.

The backups are created in a locked room, write protected, then placed in a container received from the storage facility vendor. The box is then sealed and secured in the authorized storage room that only authorized personnel may access (with a cipher-lock) until the courier pickup occurs. The backups are then transported securely and stored in the locked storage facility.

Integrity safeguards to ensure the data is not modified while in storage

We will enact a contract with a reputable storage facility, such as Iron Mountain Incorporated, whose services are designed to protect and preserve their client's data. According to information obtained from the Iron Mountain Incorporated website, the following is available:

"Trusted expert Iron Mountain relieves your backup burden - and risk - by vaulting your data in state-of-the-art facilities that are out of reach of natural or human threat.

To keep your data safe, when and where you need it, rigorously screened, trained staff manage Iron Mountain's supremely secure vaults and transport your tapes in equally secure, environmentally controlled vehicles. Further, Iron Mountain customizes its tape pickup, delivery, and rotation schedules to your business. Industry-driven policies deliver accountability for you and your business.

Iron Mountain's Media Vaulting is much more than tape backup. It's peace of mind - and security - for your business."[5]

Availability safeguards to ensure that backups are available when needed
The selected storage facility provides 24x7 support and is committed to next business day delivery. These delivery commitments are secured contractually with the selected facility.

Auditing process
We will audit this process by conducting random test runs. This process will include restoration of randomly selected files.

15. GENPO'S guerilla business continuity plan

To protect GENPO's assets during disaster situations that affect business operations, I recommend we implement a guerilla business continuity plan that is designed to offer protection in worst-case scenarios.

High level approach

After inventorying our business processes a decision has been made that in the event of a disaster that adversely affects our ability to provide our daycare services, a partial restoration of services will be undertaken. Due to the complexity of the existing systems, in recovery mode, we will not attempt to enable the web commerce functions of DTS. While on a BCP footing, tuition payments will be accepted via personal check or credit card transaction multi-part forms. Neither will we restore web portal access to DTS. Local intranet access will still be possible but no access via internet will be enabled. Due to the criticality of the child-related medical and dietary information, critical contact information and the need to provide continued access to the check in/check out and identification database, these functions must be considered as core and will be recovered.

GENPO has established a reciprocal agreement with a large local church that has sufficient facilities to allow us to recover our operation at their location. In the event that our campus should be entirely unavailable, recovery will take place at this local alternate location.

[5] Iron Mountain Incorporated, URL: http://www.ironmountain.com/offsite-data-storage.html, (20 Nov 2004)

We will enter into an agreement with a local recovery services provider to ensure that the critical hardware systems necessary for recovery will be delivered to our recovery location within 24 hours of a declaration of emergency. Concurrent with contacting the recovery services provider, the BCP Administrator will contact the off-site facility in Jacksonville and request a complete set of our backup tapes be shipped to the recovery location. All IT personnel are required to report to the recovery location upon contact by the BCP Administrator.

Upon receipt of the replacement hardware a designated IT person will layout and establish the LAN. Because we will not be connected to the internet, there will be no need to establish firewalls, the LDAP server, routers, proxies, DNS servers and/or an IDS.

One Time Tasks

- Arrange for an alternate recovery site (already in place)
- Determine minimal hardware requirements for guerilla BCP configuration
- Establish a contract with a local recovery services provider

Repeating Tasks

- Pay annual fee to recovery providers
- Conduct periodic plan reviews and adjust as necessary
- Conduct BCP recovery exercises to test plan

Auditing process to verify the approach works

Conduct periodic BCP recovery exercises including recovery services provider and the Jacksonville storage facility. This will include actual delivery of required hardware (computing resources and network hardware) and loading backups to the new hardware. Following each audit, an evaluation will be performed and recommendation for improvements will be incorporated into the plan.

How this approach scales to cover all of IT operations and all of GENPO

The basic plan methodology will be applied to other areas of GENPO, such as, the finance and materials management systems.

16. References

1. "Webopedia", URL: http://www.webopedia.com/TERM/P/POP2.html, 21 Nov. 2004

2. "Release Notes for Cisco VPN Client for Windows, Release 3.5.4", URL: http://cisco.com/en/US/products/sw/secursw/ps2308/prod_release_note09186a0080104e35.html, (21 Nov 2004)

3. Symantec Expanded Threat List, 12 November 2004. URL: http://www.symantec.com/avcenter/expanded_threats/virus_worm_trojan_horse.html, (21 Nov 2004)

4. Datz, Todd. "Trash Talk." CSO THE RESOURCE FOR SECURITY EXECUTIVES. Volume 3 Number 11 (2004): Pages 60 – 62.

5. Iron Mountain Incorporated, URL: http://www.ironmountain.com/offsite-data-storage.html, (20 Nov 2004)