Global Information Assurance Certification Paper

Michelle McCabe
Submitted December 29, 2003
GISF+ Practical Assignment
Version 1.0
Can an old security dog teach new tricks to a dog treats business?

This paper is an overview of the Hound Dog Bakery, a company that specializes in dog treats. The recent hire of me, Mutt Jones, has led the Computer Operations Manager to request that I perform an assessment of the company's computer operations and address any security vulnerabilities the company may have.

DESCRIPTION OF THE HOUND DOG BAKERY

GIAC Enterprises is the parent company of the Hound Dog Bakery. The Hound Dog Bakery is a gourmet dog treats company that presently has thirty stores in thirteen states and is considering expanding to the European and Asian markets. The company also has an e-commerce website that generates sales. The combined sales from e-commerce and mortar and brick stores total $5 million dollars.[1] The company also has a distribution warehouse that provides service for all thirty stores, as well as responding to e-commerce sales. The distribution warehouse also contains the corporate headquarters.

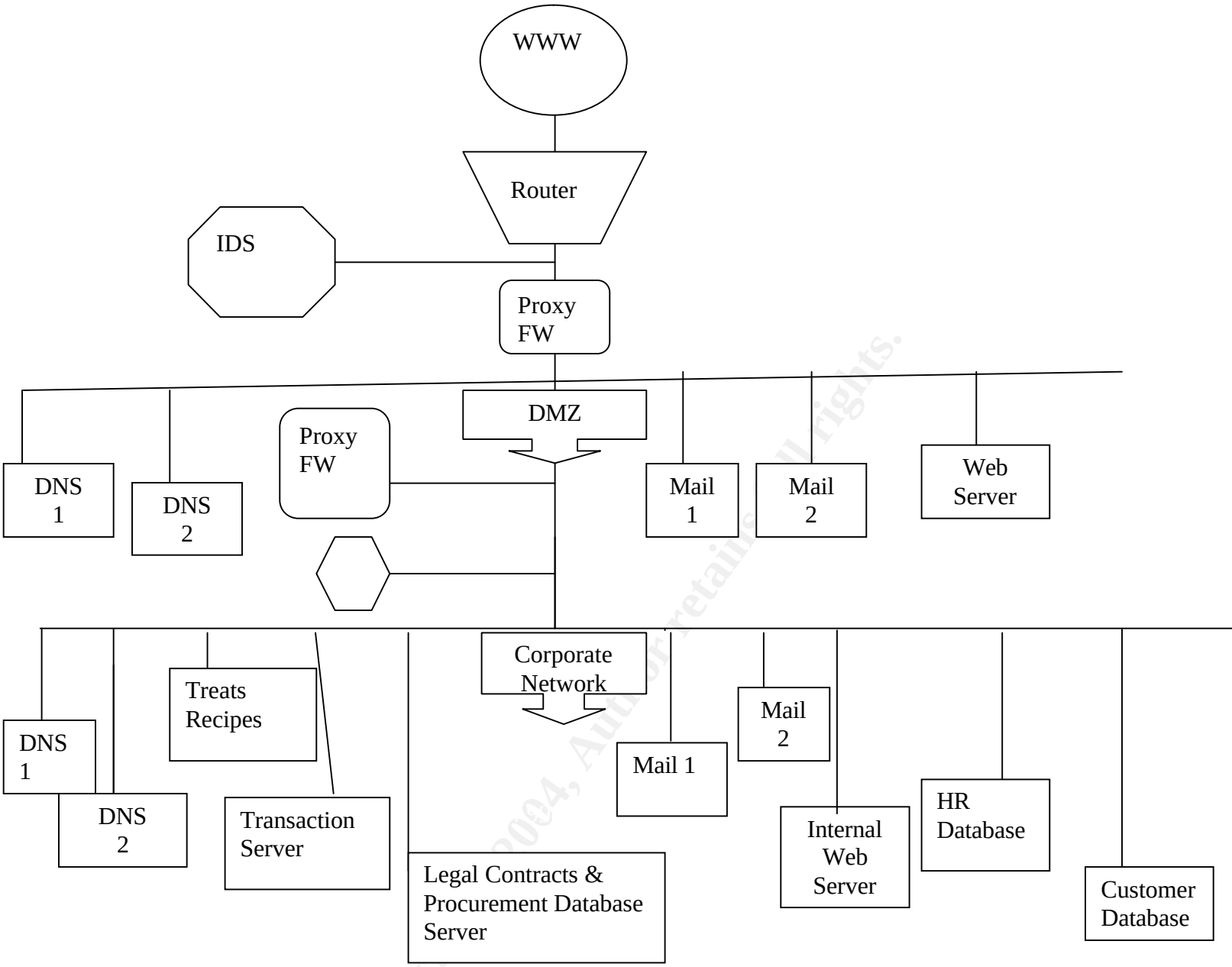
The company has 30 stores that all feed into the corporate headquarters located in Richmond, Virginia. The corporate headquarters is where the computer operations center is located.

The Hound Dog Bakery employs approximately 300 employees who are located within the company's various stores, as well as the corporate office. Store managers make approximately $35,000 a year, where as those in the Computer Operations center make approximately $50,000 + per year. Senior level executives in the company make $80,000 + per year.

NETWORK DESCRIPTION OF THE HOUND DOG BAKERY

The Hound Dog Bakery Network has each of its 30 stores connecting into the corporate network. These connections are achieved through VPN connections. For the most part, the network has been developed using the principal of defense in depth, a security layering affect, to protect the most valuable resources within the corporate network. A router assists with traffic flow at the entry point to the DMZ. Proxy firewalls and an Intrusion Detection System (IDS) are tools used to help protect the network. Each server has a tape drive for backup. Redundancy has been built in for the DNS and mail servers. All crown jewels are protected within the corporate network. We also utilize software to protect us from harmful viruses. The following diagram shows the overall view of the Hound Dog Bakery Network.

[1] http://www.wellsfargo.com/biz/products/resources/advisor/archives/01gree/01gree.jhtml



Computer Operations Division Description

The mission of the Computer Operations Division (COD) is to provide technical support and network security to the various business units of the Hound Dog Bakery.

The COD is responsible for installing, upgrading and the maintenance of all computers, electronic equipment and computer software for the various business units for the Hound Dog Bakery.[2] The division is also responsible for the development and maintenance of all web applications and web sites. The division also maintains the Wide Area Network (WAN) and Local Area Network (LAN) for the company. Finally, the division is responsible for overseeing the security of the company's WAN and LAN.

The Computer Operations Division Manager reports directly to the company's Chief Information Officer. The COD management of all the Hound Dog Bakery's computer systems helps the various business units run smoothly, efficiently and securely. The COD has a direct impact on the company's revenues through the development and maintenance of the company's e-commerce applications on the company's web site. The COD also must keep the web site and credit card servers secure and running efficiently so that customers can buy dog treats through the company website.

The Computer Operations Division staff is responsible for all of the hardware that comprises the WAN and LAN for the company. These include all of the servers that contain the company's crown jewels. All of the engineers in the division have laptops so that if necessary, they can respond to issues while away from the corporate headquarters.

The division is comprised of firewall engineers who are responsible for the administration and security of firewalls. The division also has database administrators, as well as individuals who provide desktop support. There are also individuals who provide web site design and maintenance. There are also engineers who manage the WAN and LAN.

The Hound Dog Bakery employees a total of 300 employees within its stores and the corporate office and the company's warehouse. The Computer Operations Division employees 15 staff members and this is the primary expense found in the division's budget. The budget is a total of $1.5 million dollars. 1 million dollars goes towards the salary of the division's 15 employees. The remainder of the funds goes towards hardware and software expenses such as licensing and occasional budgeted new equipment.

[2] http://www.romepolice.com/computer_services.htm

I, Mutt Jones, am an entry level engineer assigned to the Computer Operations Division for the Hound Dog Bakery. My salary is $55,000 a year. I assist with monitoring the company's local area network (LAN) and wide area network (WAN). I am responsible for implementing good security practices for the company's network. My primary area of responsibility is working on the network's firewalls.

I report directly to the Computer Operations Manager. The whole management of the network, including the security of the network falls under the supervision of this position.

One of the main areas I am responsible for are the firewalls in the network. I am responsible for keeping the firewalls up and functioning, as well as ensuring the security of the firewalls. In the past, the company's policy has been to allow everything in through the firewalls. My job is to take a new approach and to change the company's philosophy to a default deny stance. In consultation with the Computer Operations Manager, I have developed a timeline which will be used as a measure of the success of closing down ports on the firewalls.

The second area I am responsible for is ensuring the transactions web server is secured. This web server falls in the LAN and holds customer credit card information. Presently, customer personal information, as well as their credit card information is stored in one database. My job is to address the security concerns with this current set up. The measure of success for this is the development of a proposal, approval of the proposal, and implementation of it within the 6 month deadline assigned to me by the Computer Operations Manager.

How does the Hound Dog Bakery Operate?

The Hound Dog Bakery conducts its business from its thirty stores and corporate headquarters/distribution warehouse. Each of the thirty stores bakes and packages dog treats in the store. The distribution warehouse takes in orders from the Hound Dog website and processes the electronic orders. The warehouse bakes, packages, and ships treats to the company's web based customers. Management functions for the business are handled through the corporate headquarters.

Necessary applications for the business to run

Since a large part of the company's sales happen through the Hound Dog Bakery's website, it is vital that the website be reliable and secure. This means that the application server which is located in the company's DMZ must be functioning at all times. Other interactions with customers can take place through the company's help desk if they have a question or concern. The help desk must

be able to access customer's information in order to assist with customer's issues.

One of the most important databases that must be functioning is the dog treats recipes database. It is company policy that the recipes should only be available in electronic format through this database. If employees in the various stores or in the warehouse need to check a recipe, this database must be made available.

Internet access has been granted to employees who are at the corporate headquarters and has been limited to only store managers at stores.

The various store locations need to access the corporate network and do so through a VPN connection. These connections are vital for the communication of the stores to the corporate network. VPN connections have been limited to use only by store locations and executives who been approved by the Computer Operations Manager, as well as approved Computer Operations staff.

Not only is the VPN connection vital for users, but also the use of e-mail within the company. Store managers use e-mail to communicate with headquarters, and e-mail is also heavily used by the executive team for the company.

The company's policy on employee access has been to limit access to only the applications that are directly related to the employee's job function. For example, a baker at a store could not access any of the company's legal contracts or procurements. Various levels of access have been created and access can not be changed unless proper authorization has been given. In order for an employee's access to change, the Computer Operations Division Manager must receive, in writing, a change of access request form that has the signature of the Human Resources Manager, as well as the signature of the employee's manager. This checks and balance system prevents employees from inappropriately requesting higher access.

Most interaction with suppliers takes place via email, so the Hound Dog Bakery, at this time, does not have to deal with outside connections from suppliers.

The Hound Dog Bakery knows that the most important thing for the company's success is its customers. With this in mind, the customer contact lists the company has are extremely important and have been given a high priority for protection. Presently, the customer contact lists are stored in an Access database that is password protected. The marketing department and the customer service help desk utilize the contact lists. Both of these departments have access to the lists. The marketing department has read only access, while the customer service help desk has the ability to go in and update customer records. An audit trail is kept for each customer service representative who accesses and updates any records. Logs are also kept for those in the marketing department who access customer records.

Another two areas that have been identified as extremely vital are the company's contracts and procurements. The attorney's and their assistants in the legal department have complete access to the drafts and final contracts that are created. Contracts are developed in Microsoft Word, printed off in hard copies, and then signed by the appropriate authorities. Once contracts are completed, the hard copies are scanned into a database, as well as burned onto cds for backup and disaster recovery purposes. The cds are stored off site and the scanned copies are housed in a password-protected database on a secured server.

Other information that must be have limited access by employees include things like background checks, salary, performance and awards. The Human Resources Department develops salary and performance information. Performance and salary information is collected in hard copy from managers and then scanned into a database that is only accessed by authorized employees in Human Resources. Background investigations are also coordinated by the Human Resources Department and are maintained in personnel files that are kept in locked file cabinets. Only the Human Resources Manager, the Human Resources Assistant Manager and the employee who performs the background checks have access to these files. Award information is also created in Microsoft Word by managers and is then put in a hard copy format and stored in employee's personnel file in a locked file cabinet, which is located in the Human Resources Office.

One other crown jewel that the Hound Dog Bakery must protect is customer information. This information includes not only customer contact information, but also credit card information as well. Customer information, as stated above, is stored in an Access database that is password protected. Transaction and credit card information is stored in a separate database that is password protected. At this time, Customer Service Representatives have access to both databases.

After identifying crown jewels that are important to the company, the next step is to address threats to those assets. The first one to address is the access to customer data. All customer service representatives have access to the customer contact database and have the ability to go into the database, as well as the ability to update the information contained in the database. The motivation for them to change the customer contact information in that database, or the information in the credit card/transaction database would perhaps be if they were a disgruntled employee, or they wanted to commit identity fraud. The IT Support Services area has access to the customer contact information database and the credit card/transaction database through the administrator passwords they have to both databases, as well as the server where the database is located. The motivation for someone from the IT Support Services area to copy, modify, or destroy this database would be potentially a disgruntled

employee, or someone wanting to commit identity theft. This is considered a medium threat vector.

The next area to consider is the threat to the legal contracts and procurement documents. The attorneys and their legal assistants are the only authorized employees who can create and access contracts. The IT Support Services staff has access to the server where the completed contracts have been scanned in to be stored. Staff from either the Legal Department or the IT Support Services area could access the contracts and make changes to the contracts. This would involve an elaborate plot to digitize the signatures and to get them attached to the new version of the contract. The motivation for changing a contract could be a financial reward to the employee from one of the parties in the contract who would benefit from the contract modification. This is not considered a high threat vector.

Management information is the next area that needs to be addressed for threat considerations. Salary and performance information are created in a hard copy format and then scanned into a database. There is a low threat vector for these documents to be changed. Background investigation paperwork is all in a hard copy format and is stored in a locked file cabinet that can only be accessed by the investigator who performs the investigations, the Human Resources Manager and Assistant Manager. Access to these files could be gained if the investigator left the files out of the cabinet. Any of the employees who have access to these records could be a threat to copying, modifying, or destroying them. Their motivation for performing any one of these actions might be to gain a financial reward from someone who would want to access or modify the records. This is considered a low threat vector for our company.

The final crown jewel that needs to be considered for threats is the customer credit card database. Presently, staff from the Computer Operations Division can access the credit card database through the administrator passwords they have. They can also access the customer's information database. The customer service representatives currently have access to both databases as well. Staff members from either the customer service area, or the computer operations division could steal information from both databases to commit identity theft. AT this time the company thinks this is a medium to high threat vector.

Now, I will address the threat from outsiders to the Hound Dog's credit card information. The Customer Service Representatives currently have access to customer contact information and can edit or delete information. They also have access to the customer credit information. If an outside attacker was able to email to any of the customer service representatives a Trojan which logs key strokes, they could gain passwords to access customer information and their credit card information. They could either modify, or destroy the information in the databases. Or, they could steal the information to use to commit identity theft

crimes. Due to the filtering software we currently have on our network, which is updated regularly, we consider this to be a low threat vector.

The Hound Dog's network is susceptible to attacks from outsiders via the use of email. Since this is the primary way our organization interacts with those not within the corporate network. This is especially true for the customer service representatives who use email as a way to converse with customers. Looking towards the future at changes that may be implemented into the network, the network may become vulnerable to exploits such as the W/32MiMail.J exploit. This exploit comes as an email and identifies that it is from Paypal. The email says that if information isn't confirmed, the Paypal account will be terminated. If this email was sent to the customer service representatives and they responded with the appropriate information, it could allow an outside attacker access to the company's PayPal account. This would be extremely harmful to the Hungry Hound Bakery since about half of the revenue for the company comes in through the company's website.

The most sever threat to the company has been identified as credit card theft. This threat could come from either inside the company or outside the company. The chances of this occurring are considered high. The Federal Trade Commission has survey information which indicates that identity theft is on the rise. [3] Since almost half of the sales for the Hound Dog Bakery occur through our web site, we have thousands of credit card transactions that could be a target by hackers.

If customer credit card information were stolen, it would be devastating to the company in a number of ways. Not only could the Hound Dog Bakery face the loss of thousands of dollars, but the company would also be damaged publicly from the bad publicity we would receive because of a break in. Due to the recent passage of legislation in California, there could be some legal issues involved if we had customers in California whose personal information was stolen.[4]

The suggested course of action to reduce the risk of credit card information being stolen is to utilize a service such as Pay Pal. Pay Pal will allow us to implement a separation of duties, as well as customize the level of access each customer service representative has to credit card transactions.[5] While this solution is not 100 percent perfect, it will give us a better handle on credit card transactions and the logging and audit process needed to ensure the security of the transactions. Weighing the risks involved and the gains to be earned, this solution is the best fit from a security and fiscal standpoint for the company.

The implementation of this remediation strategy can best be achieved by establishing a separation of duties for the customer service representatives by

---

[3] http://www.ftc.gov/os/2003/09/synovatereport.pdf

[4] http://www.forbes.com/technology/newswire/2003/07/01/rtr1016896.html

[5] .http://www.paypal.com/cgi-bin/webscr?cmd=p/sell/permissions-outside

separating access to customer contact information and credit card information. Separating the customer's personal information from their credit card information will make it more difficult for identity theft to occur. Procuring services from Pay Pal will allow the Hound Dog Bakery to implement the separation of duties with the customer service representatives easier.

In order to get this remediation strategy implemented, a project manager should be appointed from the Computer Operations Division (COD) to oversee the project and a project team. The project team will consist of representatives from COD, Finance, and Customer Service.

The project manager will begin the process by working with the Finance area to setup an account with Pay Pal. It is estimated that it will take two weeks for the finance area to setup a Pay Pal account.

While the finance paperwork is being completed, the Computer Operations Division will create a key number to tie the credit card transactions database to the information from the customer's personal information database. The two databases will have a common customer number as a reference for correlation of the databases, as well as customer problem resolution. The internal credit card transaction database will work in conjunction with the service offerings from Pay Pal. The database reconfiguration will take approximately two weeks. Work will begin as soon as possible to have the database changes made prior to the completion of the paperwork by the Finance Department.

The manager of the Customer Service Department will need to work with the project manager to reorganize the Customer Service Representatives so that they will have a separation of duties. One group will have access to the database that will contain customer information. The other customer service group will have access to the customer's transactions and credit card information.

Once the Pay Pal setup is completed, the Customer Service Representatives will receive training on the new process. The training will be setup and coordinated by the project leader, in conjunction with the Customer Service Manager.

As mentioned above, a project team will be created which consists of a project leader, as well as representatives from the Computer Operations Division, Finance, and Customer Service departments. Each of these representatives will complete the necessary work in their areas to complete the project. The members of the project team are worker level employees. The project team leader is a management level person with training in project management.

The representatives from the COD include programmers/developers, security representatives and network engineers. These are all entry level employees. To implement this remediation there are currently no hardware or software procurement costs associated with this project.

Pay Pal will charge our company to utilize the service of accepting credit cards through them. There is no set up fee. The use fee for Pay Pal is 2.9% + $0.030 USD.[6] This fee is for U.S. dollars. The Hound Dog Bakery does not accept international orders at this time.

Hound Dog's Backup Strategy

The current problem the company is experiencing is that executives are not backing up information that they save to their local drives. In order to protect the data of Hungry Hound executives, as well as local desktop personal computers located in stores, the Computer Operations Division recommends implementing a solution by Veritas. The Veritas Backup Exec 9.1 for Windows Servers will achieve our goal and allow us to develop a comprehensive backup program. Local desktop pcs, as well as executive lap tops will all be able to be backed up through this centralized system. The Veritas software will be programmed to go out to local pcs and to back up local information to network servers. This will be done on a nightly basis. The enterprise back ups will occur on a nightly basis also. These will be scheduled at different intervals and can be scheduled through the Veritas software. Between the hours of midnight and 5 a.m. are the most inactive times for the network, thus the backups will be scheduled during that time frame. Backups for the DMZ servers will occur on a nightly basis as well.

The Veritas Backup Exec 9.1 software is priced at $795.00.[7] Since we already have tape drives that handle the enterprise backups, the new software will work with this system. No new hardware purchases will be necessary.

Presently the enterprise backup tapes are changed every other day. Since the local backups will be tied into the enterprise system, nothing will change as far as the schedule goes for changing out the tapes. The tapes are currently labeled and stored and stored in a locked file cabinet that is located in the Computer Operations Division. The file cabinet is in a room that contains fire suppression equipment in the event there is a fire.

After reviewing the needs of the company for data backups, the Hound Dog Bakery will be working towards an implementation plan to have all local drives backed up to network servers on a daily basis. With this in mind, the focus of offsite backups will definitely include all the information from our crown jewel servers located at the Hound Dog's Headquarters. We will procure the services of a company such as Iron Mountain that can provide off site media storage.

The following have been identified as one time tasks that are needed to begin the process:

---

[6] http://www.paypal.com/cgi-bin/webscr?cmd=_display-fees-outside

[7] http://store.veritas.com/searchresults.asp?dept_id=7

- Procuring the services of Iron Mountain
- Establishing staff to manage the backup process
- Development of policy and procedures for offsite backups

The following have been identified as reoccurring tasks that will be needed to continue the process:

- Procuring extra backup tapes
- Staff oversight of backup process and weekly tape pickup by Iron Mountain
- Annual review of policies and procedures on backups

We have identified that customer's personal information is extremely sensitive therefore; we do have concerns about the integrity and confidentiality of tape backups not being breached. Iron Mountain guarantees the protection of our data through the use of their state of the art facilities. The vaults they use are "away from flood planes, high crime areas, industrial rail road lines and other potential hazards."[8] Not only does Iron Mountain guarantee our information will be safe, but they guarantee it will be protected from being tampered with or destroyed. A breach of contract will also need to be included in the procurement with Iron Mountain.

Even though safeguards for the data may be guaranteed, in the event of a disaster, we do need to consider the availability of the data. Iron Mountain's program guarantees that in the event of a disaster or an interruption in business, they will guarantee that emergency retrievals will be shipped for next morning delivery. Access to backup materials is guaranteed 24 hours, 7 days a week, 365 days of the year. Even though using one company to provide backup storage resources is a risk, this level of risk is an acceptable one for the Hungry Hound Company.

Once this off site backup process has been established, it will be important to audit the process to ensure the effectiveness and security of the process. One tool we will have is Iron Mountain provides activity audits and they will follow our prescribed policies and procedures. This process will also need to be audited on a yearly basis by an outside security partner. I also recommend that the process be audited on a quarterly process by someone within the Hungry Hound organization.

Now that the threats and vulnerabilities have been addressed, it is important to discuss how the business would respond to a catastrophic event. The business does have some positives in its favor. Having 30 stores in thirteen states is an asset. Since the stores are geographically disbursed, this could be used as an

[8] http://www.ironmountain.com/File_Uploads/Resource_Items/USA/424_0_IMOSDP-OSV-0102.pdf

advantage in the event of a disaster at a specific store location, or even if there was a disaster involving the corporate headquarters. The likely hood of a disaster that would impact all 30 stores is very low. Another plus for the company is that the corporate network itself is not a complex one. In the event of a disaster, arrangements could be made to have the network back up and running.

One proposal for business continuity is to put back up servers in some of the various store locations. In the event of a disaster at the corporate headquarters, these servers could be activated to get the company network back up and running. Enough servers could be purchased to have the whole network back up, or it could be limited to only those applications that are identified as critical.

Since approximately half of the company's revenues come from Internet sales, it is imperative that the web application server and the credit card transaction servers work. Even though we will have our backup tapes stored off site by Iron Mountain, if the hardware is destroyed, we will need to have alternate hardware for the process to work. That is why I recommend that a web server and credit card server be stored at alternate store locations in the event that a catastrophic event happens to the company headquarters.

The initial tasks that would be needed to begin the process are as follows:

- Recognize the need for continuity planning for all stores as well as the corporate headquarters
- Put one person in charge of the continuity planning process
- Establish a continuity committee that has representation from different areas of the company
- Alternate work locations need to be identified
- Key personnel need to be identified
- Alternate modes of communication need to be identified
- Management needs to identify what is an acceptable amount of down time for the company's network to not be available

The recurring tasks that have been identified to keep the continuity plan going are as follows:

- Budget funds need to be allotted for continuity
- The plan will need to be tested on an annual basis
- Threats need to be reviewed and potentially new threats identified
- Contact information for key personnel needs to be kept up to date
- The continuity committee should meet on a quarterly basis to review the continuity plan
- After each test of the plan, the continuity committee should meet to review "lessons learned" from the test

In order to ensure that the continuity plan works as expected, the plan will need to be tested, at the very minimum, on an annual basis. This process should be audited by an independent firm.

By putting servers in the geographically disbursed store locations, the Computer Operations Division can have the company network functioning. In the event a store location is destroyed, a laptop can be given to the store manager so that they can keep in touch with the corporate headquarters.

If a store is destroyed, it will be more difficult to continue business continuity at a store location. One solution is the bakers from the destroyed store could be transferred to the company's warehouse and they could work night hours in order to bake treats for the destroyed store. An alternate sales location could be established that would allow for the continued sale of dog treats in the area of the destroyed store. The other alternative would be to find an alternate bakery worksite in the area where the baking of treats could resume. This would be a costly process since all new equipment would be necessary in order to setup an alternate site. Any of these scenarios can be implemented; it will be a management decision on how far they would like to go in implementing them.

Works Cited

"Compliance challenges seen for Calif. hacking law". Forbes.com. 7 July 2003. Reuters. 10 Oct. 2003 <www.forbes.com/technology/newswire/2003/07/01/rtr1016896.html>

Computer Operations Division. Rome Police Department. 10 Oct. 2003. <http://www.romepolice.com/computer_services.htm>.

Iron Mountain – Services. Iron Mountain. 23 Dec. 2003. <http://www.ironmountain.com/File_Uploads/Resource_Items/USA/424_OIMOSDP-OSV-0102.pdf>

PayPal – Use Multi-User Access to maintain internal controls. 23 Dec. 2003. Pay Pal. 23 Dec. 2003. <http://www.paypal.com/cgi-bin/webscr?cmd=p/sell/permissions-outside>

PayPal – Fees. 23 Dec. 2003. PayPal. 23 Dec. 2003. <http://ww.paypal.com/cgi-bin/webscr?cmd=_display-fees-outside>

Synovate. Sept. 2003. Federal Trade Commission. 21 Dec. 2003. <http://www.ftc.gov/os/2003/09/snovatereport.pdf>.

The Veritas Online Store – Search Results. Veritas 21 Dec. 2003. <http://store.veritas.com/searchresults.asp?dept_id=7>