Global Information Assurance Certification Paper

GIAC Enterprises
ISO Assignment 1.2

Author: Mike Butorac

Date: June 2002

Contents

Assignment 1 – Describe GIAC Enterprises

Description of GIAC Enterprises

GIAC Enterprises is a large regional bakery operating in the US Pacific Northwest. It has been in business for over forty years. It operates a central bakery, producing a wide range of baked goods, from general consumer products: white, brown, rye, etc., to various types of buns. GIAC also produces a range of dessert products, from single serving snack cakes, to large party size cakes and tortes.

Twelve regional plants produce a subset of the entire product line as appropriate for the region. A frame relay network connects these plants. All Internet traffic goes through the network in the main plant.

When the bakery first started, it was just a small retail location, with a small production area in the back of the store. Customers were all walk-in. Today, the customer base varies from small independent retail locations, small national chain stores, to large national grocery chain stores and "big-box" wholesale outlets. A home service division also operates from the main plant.

Production is a 7x24 operation, and involves maintaining a large fleet of vehicles for both the import of raw flour, other ingredients, and the delivery of finished goods in both large and small quantities.

Remote sales staff and employees working occasionally from home use the VPN.

Financially, GIAC is doing well, but senior management views the business as "simple bakers of bread", and that flashy IT systems are the domain of hi-tech companies. GIAC is very cost sensitive. This position is softening as positive results from systems like web based home service customer access begin to emerge.

IT Infrastructure

The following table lists core services and components:

Device	Hardware	Detail
ISP Router	Cisco 3620	Provided by local Telco; no customer access
Firewall	Cisco PIX 520	Software rev. 5.2(5); 128MB RAM, 16MB Flash
VPN Concentrator	Cisco 3005	Software rev. 3.5.2
Internal Router	Cisco 3640	Software rev 12.0(5)

Web Server	Dell Poweredge 2500	MS Secure IIS; 128 MB RAM
DMZ DNS	166MHz PC	Win2K Server; DNS; 96MB RAM
Internal DNS 1	Compaq Prosignia 500	NT4; SP6; 128MB RAM; DHCP; DNS; WINS
Internal DNS 2	Dell Poweredge 1300	NT4; various hot fixes; 256MB Ram; DHCP; DNS; WINS
RAS Server	133 MHz Pentium	NT4; SP6; 96 MB RAM
Proxy / Web Filter	Dell Poweredge 1300	NT4; SP6; some hot fixes; MS Proxy Server 2.0; SP1; Websense Enterprise 4.3.1; 328 MB RAM
Mail Server	Dell Poweredge 6300	NT4; SP6; some hot fixes; 1 GB RAM; MS Exchange 5.5
Mail Relay Server	Dell Poweredge 2400	NT4; SP6; Some hot fixes; 512 MB RAM; MS Exchange 5.5; ClearSwift Mail Sweeper for SMTP
Monitoring PC	677 MHz Dell PC	Win 2K Pro; 128 MB RAM; Solarwinds Engineers Edition for syslog
SQL Server	Dell Poweredge 4300	MS SQL Server 7
Intranet Server	Dell Poweredge 2400	NT4; SP6; IIS 5; 256MB RAM

Operational Notes:

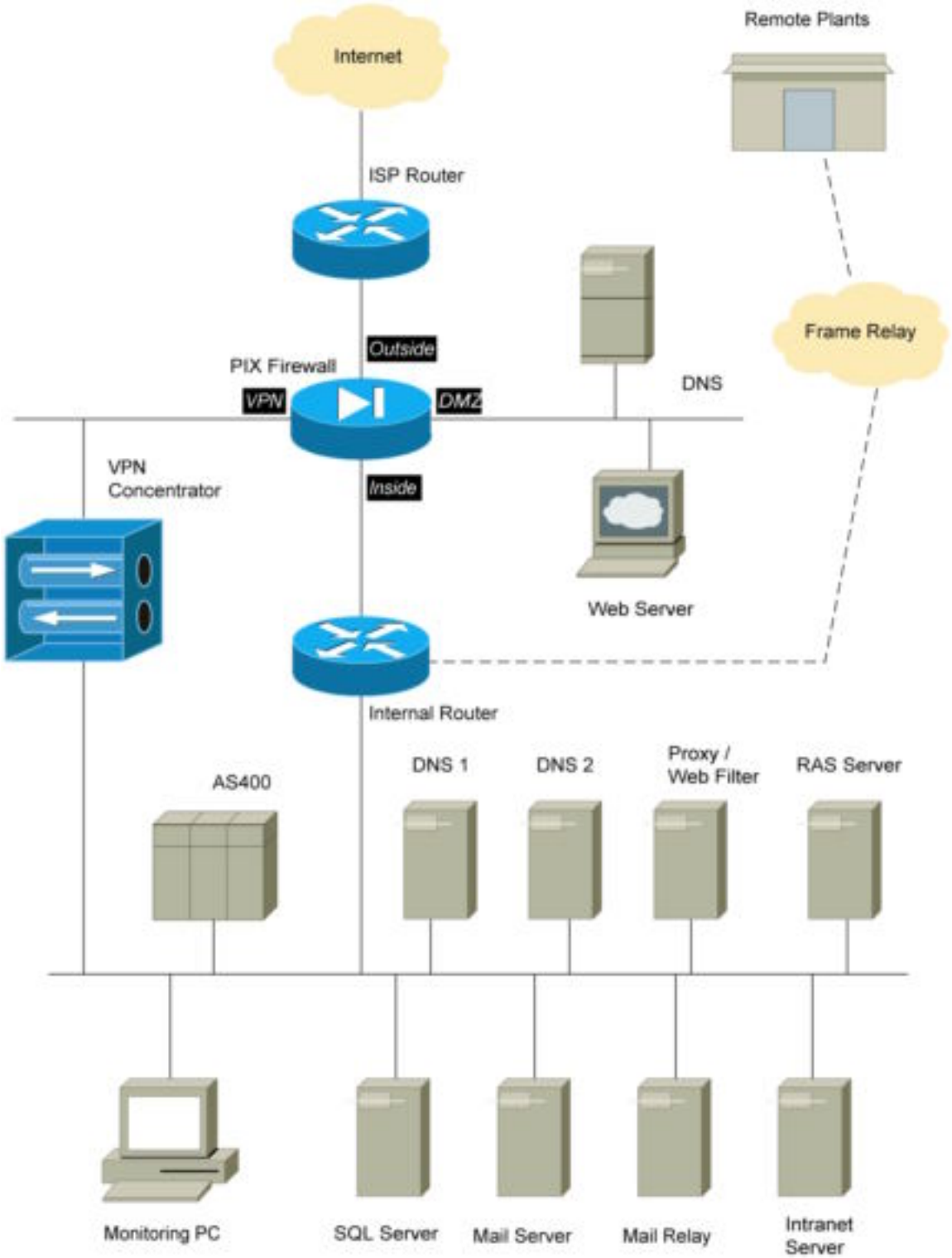
All servers and desktop computers are protected by Norton Anti-Virus Corporate version. Desktop machines are scanned daily at 5pm. Virus definitions are checked daily.

The inside LAN segment is primarily a shared, not switched environment. Some, but not all of the core servers are on a switch, but other servers and most of the client workstations are on a shared Ethernet segment. Only one subnet is in use.

The DMZ LAN segment is also on a shared Ethernet segment.

The monitoring PC is the personal workstation of one of the administrators. Full monitoring impacts performance of the machine, so the entire suite of monitoring package is not used. It was also noted that a number of servers are configured to send traffic to hosts and subnets that no longer exist. This creates a large volume of false positive traffic from the firewall on the syslog server.

Network Diagram



Business Operations

To produce a range of products that must be of a consistent high quality, GIAC Enterprises relies on its IT infrastructure to provide the tools that allow employees to work together as a team.

Inventory and Scheduling

The inventory and scheduling group have the ability to work with suppliers to ensure an appropriate amount of raw goods based on the anticipated amount of production. This is especially important since the raw goods are usually both perishable and subject to uncontrollable factors like the weather or other conditions on local farms. Electronic mail is the primary tool to maintain contact with local suppliers.

Location and staging of inventory is important to ensure the timeliness of production. Access to planning tools on local servers is key.

Finally, the inventory and scheduling group are responsible for ensuring that all activities related to shipping product run smoothly. This requires co-ordination with sales, GIAC delivery trucks, and customer trucks. Again, electronic mail plays a large role.

Sales and Marketing

The Marketing team for GIAC Enterprises relies heavily on a wide range of off-the-shelf products for the design of advertising material. These tools are located on local servers and must be available at all times. Many valuable ideas occur at odd hours so the staff must be able to use the VPN to access and update information wherever and whenever an idea strikes.

The Sales team also relies on commercial products as well as a wide range of productivity tools like PDA's. These devices all need to be able to synchronize with the core servers. Electronic mail is heavily used to communicate with customers.

Another valuable resource is the web server located in the DMZ. Besides the corporate Internet presence, the home service web site is located here. Home service customers can sign on and order product, change standing orders, and access their account information located on an SQL database on the inside network. GIAC feels that maintaining this kind of service is a very important part of business operations.

Production

Besides the standard production responsibilities of actually baking the product line, the production team also encompasses the R&D unit. This team has two primary responsibilities. The first is the maintenance of the recipes used to produce the product line. The second is the development of new products.

The maintenance of the existing recipes is critical because of the impact of a change in consistency of any product. Even the slightest error would result in a

loss of consumer confidence in the entire product line. These recipes are located on the intranet server. Access is restricted to authorized personnel only. Slight adjustments are not unusual to account for varying characteristics in the base ingredients.

The R&D unit is responsible for the development of new products. The industry is highly competitive and the development of new products is critical for the continued profitability of the company. New recipes and test results are considered extremely confidential. Again, secure intranet access is key.

Assignment 2 - Identify Risks

The purpose of this section is to identify the three most critical areas of risk to GIAC Enterprises. Although many risks may exist, dealing with the three largest risks will do the most to ensure the continued business operations of GIAC Enterprises.

Compromise of Intranet Server

As the "crown jewels" of GIAC, the integrity of the recipe information contained on this server is critical to the continued business operations of GIAC. The compromise could be the result of an external hacker, or by a disgruntled employee.

If the intranet server was to be compromised, and the data altered, deleted, or forwarded to unauthorized personnel, the potential loss would be incalculable. A slightly altered recipe would impact the consistency of the product. This would cost the business by increased production costs incurred by re-doing the production run, with the resulting delay in delivery. Even worse, would be the loss of consumer confidence. If the recipe were to be forwarded to a competitor, that competitor would possibly be able to market a competing product at lower cost.

A vulnerability that makes this risk very real is the location of the mail relay server. Mail from the Internet is directly passed through the firewall to the internal network at this point. If a hacker were to gain control of this server, it could be used as a base to launch attacks on the intranet server.

Although this server does run ClearSwift Mail Sweeper for SMTP, a new virus could get through before an anti-virus update can be developed. For an example of the changing nature of viruses, please read the following news report by Robert Lemos detailing a new virus type.

http://story.news.yahoo.com/news?tmpl=story&ncid=73&e=2&cid=73&u=/zd/20020613/tc_zd/935766

Since the threat to the intranet server comes from two sources, two different courses of action are recommended to mitigate the risk.

To deal from the threat posed by hackers, the following steps are recommended:

- Move the Mail Relay server from the inside subnet to the DMZ.
- Replace the hub currently in use in the DMZ with a 10/100 switch.
- Implement a VLAN scheme to isolate the servers located there.
- Ensure the firewall is correctly screening traffic for mal-formed SMTP packets.
- Implement an Intrusion Detection System. Locate it on the inside LAN, and place a sensor in the DMZ.
- Ensure that the server OS is hardened. There does not appear to be a coherent policy of ensuring that servers are running the most current patch level.

To deal with the threat posed by unauthorized internal users, the following steps are recommended:

- Replace the hubs currently in use on the LAN with 10/100 switches.
- Implement a VLAN scheme to isolate the intranet server.
- Use one server for sensitive recipe information and another for the general internal company related material.
- Implement and enforce a strong password policy.
- Enable auditing on the intranet server.
- Enable the scanning features of Websense to scan outbound email for keywords related to the sensitive information on the intranet server.
- Implement a RADIUS server to track authentication, authorization and accounting (AAA) for the intranet server.
- Make specific reference to the information on the intranet server in the Acceptable Use Policy.
- Ensure the intranet server is protected by appropriate physical security.

Compromise of DMZ Web Server

Besides presenting GIAC Enterprises to the Internet world, this web server provides access to customer information located on the SQL server on the inside LAN. An attack on this server by hackers could impact the business in different ways. A Denial of Service type of attack would make customer access difficult, if not impossible. Loss of revenue would be the most immediate result. A decline in customer confidence would result if this attack were to be publicized.

A compromise of the server would result in the access of customer account information. The release of this information could be very damaging to the company. Please go to the following report by Kevin Poulsen on the effects of exposing customer data for more. http://online.securityfocus.com/news/431

To mitigate the risk presented by compromising the DMS Web Server:

- Replace the hub currently in use in the DMZ with a 10/100 switch.
- Implement a VLAN scheme to isolate the web server.
- Ensure that the server is hardened and all patches applied properly.
- Ensure that the web server processes all incoming data before passing it through to the SQL server. This will ensure that the web server is not acting as a simple relay or reverse proxy.
- Force a high level of security on client web browsers.
- Monitor system logs on a regular basic for evidence of attempts at penetration.

- Correct problems on all other machines that are resulting in current syslog false positives.
- Clearly post security warnings on the web application start page advising that unauthorized access is not permitted, and that all traffic to the web site is logged.
- Develop a formal emergency response procedure.

Extended Damage to IT Facilities

As detailed throughout this report, GIAC Enterprises relies heavily on its IT infrastructure. With GIAC being located in an active earthquake zone, the risk of a severe, business disrupting earthquake is a distinct possibility. Please refer to Richard Stengers' article on earthquake risks in the region for more information: http://www.cnn.com/2001/TECH/science/03/01/quake.folo/.

For specific information on business impact, please read the following article from CNNMoney: http://money.cnn.com/2001/02/28/news/quake_business/.

Even if the earthquake were to result in no injuries to GIAC staff, an earthquake that severely damaged IT resources would effectively put GIAC out of business. Assuming production facilities at the main plant would be damaged, production could be shifted to the regional plants until the main plant is repaired. However, normal business activities would be severely crippled if the IT infrastructure were out of commission for any length of time.

To mitigate this risk, the following steps are recommended:

- IT infrastructure should be on a UPS, which is backed up by a diesel generator.
- The current backup strategy should be re-evaluated. Since operations are 7x24, many files and databases may be continually open. This can make backup difficult. An on-line backup system that can be used to track all transactions and re-build any damaged database quickly should be investigated.
- Select one of the other regional locations as a backup 'hot site'.
- Investigate the availability of a high-speed, managed service between the main and backup sites. Use this link to rapidly replicate data.
- Install content delivery switches (Cisco CS11000 or equivalent) at the main and backup locations. Also investigate a second; separate ISP. This will ensure high availability and redundancy of the web services.
- Ensure business continuity plans are in place and up to date. All staff must be thoroughly familiar with the BCP.

Assignment 3 – Evaluate and Develop Security Policy

Evaluation of Existing Security Policy

The GIAC Corporate Information Security Policies posted on their intranet site are used to deal with the handling of information on the intranet server. This policy was taken directly from the real company that GIAC Enterprises is modeled on. Please refer to the introductory information in Appendix 1, and the Security Policy in Appendix 2.

I will be evaluating the policy generally, and in terms of addressing the risk of the compromising of the intranet server.

Purpose and Background:

This offers a very good back background that helps to assure the reader that confidentiality, availability and integrity of information is important. However it doesn't identify exactly why any one policy is necessary, or what risks or vulnerabilities any one policy is designed to address. Taking this step will help educate and inform users about IT security and its importance to the company.

Scope:

This policy clearly identifies who in the company should be doing what. It is interesting that even the HR department is involved. They must notify the IT department of all new hires, terminations, etc., that may require a change to access privileges. This demonstrates to all that IT security is the responsibility of everyone.

Policy Statement(s):

This is a good, comprehensive list. It provides a list of things that actually need to be done by the users, management, and others. They are all clear, and include references to other corporate policies. I would suggest that the format remain constant throughout this section. For example, under the security / system administrator heading, the format switches from bullet points to a paragraph that appears to be more of a job description rather than that of a policy statement.

There is also a lack of direction on how the servers or other pieces of network infrastructure should be handled.

Responsibility:

The policy does good job here because it clearly defines who is responsible for what task. Taking the extra step of providing the name and phone number of the VP of IT as a contact for any questions or concerns is a good idea. It shows that senior management is willing to discuss IT security issues with its employees.

Action:

The policy does a good job of defining what actions can be taken to comply with the policy. For example, changing the password immediately if the user suspects that their password has been compromised.

Revision of Existing Security Policy

1. Purpose
    a. The information contained on the GIAC intranet server is considered by management to be one of the most important assets owned by the company. The integrity of this information is central to the continued operations of GIAC. Compromise of this information by outside sources like hackers or by unauthorized use by persons connected to the GIAC network is viewed as a serious issue by GIAC management. This policy is designed to ensure the security of the information on the intranet server.
2. Scope
    a. This policy will apply to all GIAC employees, contractors, and service personnel.
3. Policy
    a. Users
        i. Treat all computer login information (passwords and user-IDs) as confidential and for their own use only.
        ii. Ensure their user-ID login and password information is not shared.
        iii. Ensure their workstation is not left unprotected while logged on to the network.
        iv. Not test or try to bypass any security or to use any access codes or passwords other than those issued to them.
        v. Change their password immediately if they suspect their password is compromised.
        vi. Notify appropriate personnel if a user suspects data security is compromised.
        vii. Never use company computer resources for purposes other than the intended business purpose.
        viii. Comply with all security policies, practices and corporate code of conduct.
    b. Management

i. Ensure employees reporting to them are made aware of all security policies and encourage compliance.

ii. Request the necessary access to information resources for their employees through the appropriate administrative areas.

iii. Deactivate accounts when those accounts are going to be inactive for more than a month. This includes vacation, sick leave, maternity, etc.

iv. Provide each employee with their own unique login capability, which means not providing one login for multiple employees.

v. Specify, in writing, the assignment of ownership of responsibilities for databases, master files, and other shared collections of information. These written statements should also indicate the individuals who have been granted authority to originate, modify, or delete specific types of information found in the aforementioned information collections.

vi. Identify information, which need higher levels of protection that what is considered standard.

c. Information Owners

i. Authorize and approve access to GIAC information systems or resources based only on a need to know basis.

d. Security / System Administrators

i. The intranet server containing sensitive information will be installed in such a way as to eliminate any traffic not destined for that particular server. Separate VLAN's or subnets would be acceptable methods.

ii. Electronic systems will be used to ensure the security of the server. These systems include, but are not limited to an intrusion detection system and an anti-virus system. A designated administrator will monitor logs daily and ensure that these monitoring systems are updated regularly.

iii. All administrators will maintain a high level of knowledge of the system, and should rotate responsibilities (e.g. log monitoring) on a regular basis.

e. Human Resources

i. The HR department will immediately notify the IT department of all new hires, terminations, promotions, demotions, reassignments, leaves of absence, short or long term disability, or other significant changes in status that might

require a change in information access privileges on a timely basis.

4. Responsibility
    a. Ownership of this policy belongs to the VP of Information Technology for GIAC. The owner is responsible for the content of this policy, its maintenance and distribution. Enforcement is the responsibility of the Senior Network Administrator.
5. Actions
    a. Any change required to GIAC infrastructure to comply with this policy will be implemented within 30 days or as soon as reasonably possible.
6. Compliance
    a. The Internal Audit department will be responsible for ensuring compliance by engaging either a qualified internal member or external contractor on an annual basis to conduct a security audit. A designated system administrator will regularly monitor logs looking for violations of this policy.
7. Enforcement
    a. Persons found in violation of this policy may be subject to disciplinary action up to and including termination. Evidence of criminal activity may be forwarded to the appropriate law enforcement agencies.

Assignment 4 – Develop Security Procedures

Private VLAN Configuration Procedure

Note: I am assuming that a new Cisco switch has been purchased and installed in the DMZ to replace the hub described earlier. It is also assumed that the switch chosen is appropriate for the application and has a current software revision. I have also made up the IP addressing scheme for the purpose of this assignment. Detailed information on the use of a PVLAN is taken from the Cisco Systems publication "Securing Networks with Private VLANs and VLAN Access Control Lists".

Introduction:

Servers located in the DMZ are supposed to accept traffic from the Internet, and then, after suitable processing, initiate a session with a backend server. This backend server is the only server that the DMZ server is supposed to talk to. Since all the servers are located in the same subnet, one server has the ability to initiate layer 2 communications with another server. A Private VLAN is used to isolate servers, and prevent that communication.

The following procedure is to be performed by a network administrator to setup a Private VLAN (PVLAN) whenever a server is installed in the DMZ.

Procedure:

The following changes are required on the PIX Firewall. Bold text indicates changes to be made.

1. Port 1 is the promiscuous port for the connection to the firewall. Do not change this.
2. Connect the server to the first available switch port and note its number. For illustration, this document uses port 3/9.
3. Choose the next available VLAN number. For illustration, this document uses VLAN 42. VLAN 41 is the existing primary VLAN.
4. From an approved console session, enter enable mode.
5. The address of the internal server is 172.16.171.9. Allowed ports are TCP 80, and UDP 1645 and 1646. ICMP echo packets will be allowed.

```
nameif ethernet2 dmz security50
ip address dmz 199.5.6.10 255.255.255.0
global (dmz) 1 199.5.6.11
static (dmz,outside) 199.5.6.199 199.5.6.199 netmask 255.255.255.255 0 0
conduit permit tcp host 199.5.6.199 eq www any
conduit permit udp host 172.16.171.9 eq 1645 host 199.5.6.199
conduit permit udp host 172.16.171.9 eq 1646 host 199.5.6.199
conduit permit icmp any host 199.5.6.199 echo
```

The following procedure sets the PVLAN configuration on the Cisco switch. Bold text indicates changes to be made.

```
DMZswitch (enable) set vlan 42 pvlan isolated
VTP advertisements transmitting temporarily stopped,
and will resume after the command finishes.
Vlan 42 configuration successful
DMZswitch (enable) set pvlan mapping 42 3/9
Successfully set the following ports to Private Vlan 42:
3/9

DMZswitch (enable) set pvlan mapping 41 42 3/9
Successfully set mapping between 41 and 42 on 3/9
```

Verification

Perform the following steps to confirm your changes.

```
DMZswitch (enable) sh pvlan
Primary Secondary Secondary-Type Ports
------- --------- -------------- -----------
41      42        isolated       3/9

DMZswitch (enable) sh pvlan mapping
Port Primary Secondary
---- ------- ---------
  3/1 41      42
  3/9 41      42

DMZswitch (enable) sh port
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ ----- ------------
 3/1  to_pix_port_2      connected  41         full 100     10/100BaseTX
 3/9  server_dmz1        connected  41,42      a-half a-10  10/100BaseTX
```

Appendix 1 – Existing Security Policy Introduction

The following is from the main IT security policy page on the intranet of the real company that GIAC Enterprises is modeled on. Links from this page take the reader to the other security polices.

GIAC Enterprises recognizes that information and information technology are critical corporate assets and must be effectively and efficiently managed. Timely and reliable access to corporate information and information technology is essential to the ongoing successful operation and control of our business. GIAC is committed to safeguarding these assets in a manner and cost commensurate with their sensitivity and value.

Specifically, GIAC is committed to the following:

- Information will be readily available to all personnel who are authorized and responsible for meeting the operational, financial and decision support needs of the Company
- The integrity of information and information systems will be maintained by ensuring appropriate safeguards are in place to protect against unauthorized modification, destruction or fraudulent use
- The confidentiality of information will be maintained by controlling access and disclosure of corporate information to those with proper authorization
- Appropriate training and supporting reference materials will be made available to all users of information and information technology
- An information retention and destruction program will ensure that corporate and legal requirements are met
- In order to attain these information security objectives, GIAC has developed a Corporate Information Security Policy. This policy has been broken down into sub-topics. Under each sub-topic are specific policies and guidelines, all of which will help GIAC attain its objectives for information security.

For any additional concerns please contact:

[deleted]

Appendix 2 – Current Security Policy

This policy is the current policy posted on the intranet site of the real company that GIAC Enterprises is modeled on.

USERS

All users of the GIAC network will:

1. Treat all computer login information (passwords and user-IDs) as confidential and for their own use only.
2. Ensure their user-ID login and password information is not shared.
3. Ensure their workstation is not left unprotected while logged on to the network.
4. Manually enter password or access codes for initial login.
5. Not test or try to bypass any security or to use any access codes or passwords other than those issued to them.
6. Change their password immediately if they suspect their password is compromised.
7. Notify appropriate personnel if a user suspects data security is compromised.
8. Never use company computer resources for purposes other than the intended business purpose.
9. Comply with all security policies, practices and corporate code of conduct.

MANAGEMENT

Management of GIAC will:

1. Ensure employees reporting to them are made aware of all security policies and encourage compliance.
2. Request the necessary access to information resources for their employees through the appropriate administrative areas.
3. Notify the appropriate administrative areas immediately of all changes to access requirements such as transfers, termination, etc.
4. Deactivate log-ins when they are going to be inactive for more than a month. This includes vacation, sick leave, maternity, etc.
5. Provide each employee with their own unique login capability, which means not providing one login for multiple employees.

6. Specify, in writing, the assignment of ownership of responsibilities for databases, master files, and other shared collections of information. These written statements should also indicate the individuals who have been granted authority to originate, modify, or delete specific types of information found in the aforementioned information collections.
7. Identify information, which need higher levels of protection that what is considered standard.

INFORMATION OWNERS

Information owners will authorize and approve access to GIAC information systems for resources. Access to information resources will be based on a need to know basis i.e. what is necessary to perform your functions.

SECURITY/SYSTEM ADMINISTRATOR

Every GIAC multi-user computer system (mainframe, network, Internet, etc) should have a designated system/security administrator to define user privileges, monitor access control logs, and perform similar activities. This administrator should have proven relevant skills and qualifications in computer security administration and be approved by management. Administrators are responsible for maintaining up-to-date records reflecting all of the computer systems on which employees have user-IDs and monitor the effectiveness of information security controls. Other responsibilities will include coordination of the development of information security training and awareness classes as needed. All suspected security violations will be investigated and documented. Also, administrators will establish control override facilities and log review procedures to be used where controls must be compromised to maintain ongoing business operations.

HR

The HR department will immediately notify the IT department of all new hires, terminations, promotions, demotions, reassignments, leaves of absence, short or long term disability, or other significant changes in status that might require a change in information access privileges on a timely basis.

Appendix 3 - References

Lemos, Robert. "JPEG Worm Breaks New Ground". June 13, 2002. http://story.news.yahoo.com/news?tmpl=story&ncid=73&e=2&cid=73&u=/zd/20020613/tc_zd/935766

Poulsen, Kevin. "Qwest Glitch Exposes Customer Data". May 23, 2002 http://online.securityfocus.com/news/431

Stenger, Richard. "More quakes ahead for Pacific Northwest?". March 1, 2001 http://www.cnn.com/2001/TECH/science/03/01/quake.folo/

CNN staff and wire reports. "Quake shakes businesses". February 28, 2001. http://money.cnn.com/2001/02/28/news/quake_business/

"Securing Networks with Private VLANs and VLAN Access Control Lists". Online. Available http://www.cisco.com/warp/public/473/90.shtml