Global Information Assurance Certification Paper

GIAC WELLNESS ENTERPRISES

By: Laura Bell

Information Security Officer Training

GISO Practical Assignment Version 1.3

Abstract

This paper is to demonstrate the understanding of course materials that was studied for in the GISO Information Security Officer certification. It will describe a fictional wellness company that will be referred to as GIAC Wellness. The current state of the company will be described and then three security risks will be identified. Steps on how to improve these security risks will be outlined. A Security policy will be analyzed and discussed. Also a security procedure will be written to show how a policy is put into action.

GIAC Wellness Description

GIAC Wellness is a small privately-owned business dedicated to showing people how to lead and maintain a healthy lifestyle. The company creates nutritious but delicious recipes, gives guidance to clients to motivate them, and provides personal fitness trainers as needed, depending on what the client's goals are. The office is professionally decorated and has the feel of an exclusive spa rather than a gym. The business was started by a husband and wife team who both has a degree in nutrition and fitness. The company has been in business for five years and employees 22 people. All of the employees work out of one location. The office is located in a strip mall in an upscale suburban area just outside of a large Metropolitan area. GIAC has been able to stay in business due to their unique approach to fitness and weight loss. They have been able to put a personal touch to their business that makes it stand out from all of the other fitness centers.

The owners of GIAC discovered that most people want to lead a healthy lifestyle but lacked the support or necessary outside motivation. Most people just want to be told what to do and then get feedback and praise regarding their progress. They discovered that when another person is watching you and seems vested in you, you tend to exercise and eat the right things. This seems to work exceptionally well when a weekly visit reveals if you are following the regimen or not.

IT Infrastructure Description

This section describes the Network Infrastructure of GIAC Wellness. It also includes what security measures GIAC has taken to protect its network. See Figure 1 in the appendix for the network drawing.

- The Router is a Cisco 3548 switch. It is used to provide Private IP addressing to the internal network through Network Address Translation (NAT).

- All data that comes into the network passes through the Firewall which is running Cisco's PIX based operating system. All unneeded network traffic is blocked at the firewall.

- The Network Intrusion Detection is running Snort version 1.9.0 and it monitors the internal network and the DMZ for unauthorized activity.

- The switch used is a Cisco 3548 running IOS version 12.0

- GIAC uses Windows 2000 Active Directory as their Domain Architecture.

- The Email server used by GIAC is Microsoft Exchange 2000. The virus protection for this server is Sybari Antigen. It is configured to scan using updated patterns from Symantec and Trend.

- The servers that are in the GIAC network are all Dell 2550 Enterprises servers. They are running MS Windows 2000 Server OS. All have current service packs and hot fixes installed. All of the servers, except for the Web server are running the Norton Antivirus software.

- The file and print server is used for file storage for the entire office and also handles the printing.

- The application server stores the database where all of the Wellness menus and exercise routines are housed. It also houses other software that is utilized within the company such as HR and class scheduling software.

- The Anti-virus server is also used as a Backup Domain Controller.

- The Domain controller and backup controller are necessary for the authentication of users and other functions required for the domain. The DNS server is integrated with the Domain controller.

- GIAC's web server is located in the DMZ. It is mainly used so the public can learn more about the company, what services it provides, and how to contact them if one so desires. This server does not allow any input, but is used only for informational viewing. This server is running IIS (Internet Information Server) version 5.0.

- All workstations at GIAC are Dell Optiplex. They all have a standard image loaded on them and are running Windows 2000 with Office 2000 installed. The workstations are also running Norton Antivirus Corporate Edition client.

- Backups are performed every night automatically by a workstation located in a locked room by the IT manager's office. An incremental is performed Monday thru Thursday night, and on Friday night, a full backup is performed. The tape with the full backup is picked up every Monday and stored offsite in a locked controlled environment. The incrementals are kept in a fire safe box in the locked room where the backup workstation is kept.

- Employees are able to access their Email remotely by using Microsoft's Outlook Web Access (OWA). No other form of remote access is currently available.

GIAC Wellness Business Operations Description

GIAC started its business based on relationships it had with doctors who recommend the business to clients who had health issues due to their weight. The excellent results the company produced made them a standard recommendation. As the customer base increased, new clients come by word of mouth from other clients. Advertising in the Yellow Pages, distribution of flyers and other relationships the company had with clinics helped their business grow. The company's website also was helpful in getting new clients.

GIAC's personnel consist of the following people:

The President/CEO and Vice President are the two owners of the company.
Two HR personnel
Two dieticians who create the menus and unique recipes that are given to the clients.
Two Administrative Assistants who in addition to normal paperwork, setup appointments, maintain the office calendar, and screen phone calls.
Four counselors
Six fitness trainers
Four IT personnel: This consists of 2 desktop IT technicians and 2 Information Security personnel who all report to the IT manager.

When GIAC Wellness first encounters a client, a counselor sits down with them and conducts an in depth interview. Information such as hip, waist and chest measurements, current weight, age, and private conversations notes are input into the GIAC Wellness database. It is in this interview that the client's lifestyle,

eating habits, weigh and health goals are talked about. Much of this personal information is put into the client's electronic file in the Wellness database.

The business caters mostly to an upper-class clientele whose lives are very busy but who want to stay healthy or are trying to loss weight and need some direction and motivation in obtaining that goal. Ninety percent of the clients are women. The company is best known for the personalized diet and exercise program they design for their clients. The reason why GIAC Wellness has become so popular is due to their easy to follow step by step guideline in instructing their clients on what to eat and what specific exercises they should do. In addition to being able to exercise at home, those client who so desire can participate in the on-site classes where GIAC's personal trainers are available to instruct them on correct form and posture, as well as provide necessary but gentle motivation where needed.

Each client gets a detailed menu of food that they can have for breakfast, lunch and dinner. Combinations of menus provide enough variety for a month's time. Six different menus are rotated throughout the calendar year a month at a time, which helps keep the food choices new and desirable. The package also gives the client a list of recommended repetitions of specific exercises and how much time should be spent exercising. These exercise routines are developed by the personal trainers and are also stored in the Wellness database. Specific routines are personalized for each client depending on her profile.

When the client comes back for the weekly consultation, the counselor records what exercise they actually did and how many reps they were able to perform. All of this information is input into the Wellness program under the client's profile. A new schedule is then automatically generated that may increase the reps or add additional exercises as needed, depending on how well the client is doing. Every month a chart is printed out showing the client what goals have been met and how many inches or pounds have been lost.

The Wellness program was developed in-house by GIAC's IT manager. The client's profiles, the menu recipes and the exercise routines are all stored in this program. In addition to their client list, this data base is their "crown jewel". It is the livelihood of the business. Since quite a bit of personal information is stored in the database, the security settings are configured for least privileged access. Only the counselors are able to see the client's personal notes. Although everyone can view the menus, only the dieticians are able to make any modifications to the corresponding recipes. Only the fitness trainers can modify the exercise routines that are developed.

All of the workstations have Web access. Because of the wealth of information that is available on the Internet, all staff members access the web for research, health trends, and new ideas. There is no content filtering on GIAC's web

server, but the company has a policy in place that informs employees of the acceptable use of the Internet.

Email is GIAC's major form of communication between employees as well as communication with clients who have email addresses. Each employee has an email address and mailbox on the Email server. There is a policy in place that informs the employees of acceptable Email usage.

Access to the lobby is open during business hours when clients are coming and going. A receptionist logs all visitors in and out of the building. All of the GIAC employees have picture ID badges that have a magnetic strip on the back. This allows them in and out of the building after hours.

The servers are housed in a controlled access room that only the IT manager and IT staff can access.

Areas of Risk Identified

Three critical risks have been identified for GIAC Wellness Enterprises. These identified vulnerabilities could have a major impact to the business if they occurred.

1) Unauthorized access to the GIAC network and to the server on which the Wellness database and client list, GIAC's "crown jewels", is stored.

- What are the risks?
  - Ease of access to GIAC's network due to poor password policies.
  - The revealing of a username and password due to poor security awareness by an employee. This can be revealed either by shoulder surfing or having the password written down in a location where it can be found and viewed. According to Howard Schmidt in CISO magazine, "In many cases, the bad guys are able to compromise our networks because of poor authentication: blank or missing passwords, passwords that have been compromised through social engineering or carelessness, etc."
  - Keeping the default password on built-in accounts. These default passwords are usually known by even the most average hacker.

- Why does this risk concern GIAC Enterprise?
  - GIAC prides itself on producing easy to follow exercise routines that can be done on site or at the client's home. They also pride themselves on creating delicious but nutritious recipes. The safe keeping of the database that houses that information is of primary

concern to the company. Unauthorized access to its data by parties intending to do harm directly affects revenue flow and the client's confidence in the company on protecting their privacy.

- What are the possible consequences?
  - If the GIAC Wellness database is compromised, the result could be malicious activity resulting in the corruption or deletion of data. If appropriate files cannot be accessed, a loss of clients could occur. Even worse the private information on their clients could be revealed, resulting in legal liabilities for GIAC.

- How can GIAC Enterprises mitigate the risk?
  - GIAC's security team should implement periodic audits of file access and user accounts permission levels.
  - Implement a strong password policy to make it that much harder for a person trying to guess a password in order to gain unauthorized access to the network.
  - Conduct a security awareness program for the employees. Inform them of the consequences of "social engineering" and "shoulder surfing" which could compromise their password or reveal sensitive data.
  - Default or built-in accounts in the system should be identified and disabled or even better, removed if possible.

2) Virus Infections within the network.

- What are the risks?
  - New viruses are introduced every day. The antivirus signature/engine that is currently installed on servers and workstations can become obsolete overnight.
  - Users can open emails that have a Trojan horse as an attachment, thus putting the entire network at risk. Joel Deitch, Editor of the Connect magazine states, "Every IT administrator knows the damage that worms, viruses, Trojan horses and other attacks can do to the enterprise."

- Why does this risk concern GIAC Enterprise?
  - GIAC employees scan the web everyday as well as receive email. These are two main entry points for viruses to be introduced into their system if the workstations or servers are not sufficiently protected.

- What are the possible consequences?

- The consequence of a virus infection could mean significant downtime and data loss. While some virus do no more than rename or move files, there are some particularly malicious ones that can tie up the email system by sending mail to everyone on the address book or actually make changes to the computer's registry.
- If an infected email is sent to a client that originates from GIAC, this could cause damage to the company's reputation as not being able to filter its email. The client could become wary of future emails from the corporation, especially if the first contaminated email caused damage to the client's network.

- How can GIAC Enterprises mitigate the risk?
  - Use the automatic update feature of the anti-virus software. Also, an email should be automatically sent to an IT system administrator and any other designated person whenever a new signature is available so they can confirm the updates did take place.
  - Communicate to the employees of GIAC to use caution when opening emails from an unknown sender, especially emails with attachments.
  - Block known bad file extensions.

3) Reliable Backups

- What are the risks?
  - Incomplete backups of business critical data due to the backup program not operation properly.
  - Insufficient physical protection of the actual tapes where the backups are stored.
  - Not backing up data at a sufficient interval thus leaving gaps in data.

- Why does this risk concern GIAC Enterprise?
  - As with all businesses, there will be a time when the retrieval of data is necessary. Jayne Parkhouse of SC magazine comments, "In the IT security world, no matter how optimistic we feel, disaster may only be a short step away." This can be due to a hard drive crash, the accidental deletion of business data or some other incident. GIAC needs the ability to recover data and in a timely manner in order to continue their business.

- What are the possible consequences?
  - If an incident occurred where GIAC's data was ruined or destroyed, the company could possibly end up losing a large percentage of their clients if they were not able to retrieve the data in a timely manner. There are too many competitors in the health industry that

could lure GIAC's customers away while GIAC is trying to rebuild their database.
    - If data is not retrieved, the company could go out of business.

- How can GIAC Enterprises mitigate the risk?
    - A backup and restore policy and procedure should be created and adhered to.
    - At minimum, perform a backup up daily. Even better, a full backup should be performed weekly and incremental backups should be run every day.
    - Once a month a test of the restore procedure should be performed to confirm the backups are working correctly.
    - Provide sufficient physical protection of the backup media since they contain GIAC's sensitive business information. If the backups are kept onsite for quick retrieval to perform restores, a copy of the tapes should also be housed off-site.

Evaluate Security Policy

The policy that will be evaluated will be one concerning Virus protection. This was one of the identified risks for the GIAC Wellness Enterprise. This policy is based on a policy in use at the author's company. The full policy is included in Appendix A.

Purpose: The opening statement of this policy starts off very good. The policy purpose statement is very concise and states exactly why the document was written. The reader can easily determine what the document will cover.

Scope: Concerning the scope, the policy once again clearly and concisely states what personnel the policy applies to. It also covers what area of the company's assets should be in compliance. The statement leaves no misunderstanding of who should be following this policy.

Background: This policy does not go into the background of why this policy is needed and should be implemented. However, with the heavy usage of computer's today, even the youngest users know what a virus is and the damage it can bring. For this particular policy, a background statement for justification can be left out since it is pretty much understood why an anti-virus policy is needed.

Policy Statement: The policy statements are very good in covering in detail what the expectations are for anti-virus protection. The policy clearly requires the software to be certified. This would eliminate the purchasing of a start-up

vendor's software that perhaps could be inexpensive but not necessarily certified. The tried and true software is much more important in this area than the most cost efficient.

A defense in depth approach is apparent in the policy, as there is a requirement that the workstation and servers have different vendor's software installed on them. This fits in with GIAC's stance. Also there is detailed information requiring scanning of incoming traffic as well as blocking of certain file attachments.

The policy also addresses those situations where a business-critical server may become unstable if the software is running on it. It those cases, specific criteria is outlined in order for those servers to not have anti-virus software. This is one of those cases where the business makes the decision that the risk is low enough to bypass this security measure.

Even though exceptions are outlined for servers, the policy makes it very clear that there are no exceptions made for the workstations. These normally present the biggest risk of introducing a virus into the network so the risk would be too high to make an exception. Instead of making a general statement about desktop configuration, the policy goes into some detail as to what is expected regarding the virus protection of the workstation.

Responsibility: The policy does a good job in explaining what the responsibilities and expectations are of the user community to minimize the introduction of a virus into the network. It states specifically actions that should or should not be done to stay within compliance of this policy.

However, the policy does not address anything regarding who can draft, review, approve, or modify the policy. It appears this may be assumed to be the Information Security team's responsibility since it was originated by this group, but a good policy would state this so as to take the guess work out of who to go to when a modification or update has to be made.

Action: This policy does a good job on stating what specific actions a user should take if he or she suspects that his workstation has a virus. GIAC could benefit from the fact that users would know what to do if they did suspect they had a virus. By outlining what actions the user should take, it helps minimize the spread of the infection. There is also an implied action given to the Helpdesk as to responding to such a call. The policy also makes reference to a Virus Emergency Response Team that will handle any breakouts, but it does not state the specific actions that would take place. It would be better if the policy listed the specific document reference numbers and perhaps the documents location, so that when an outbreak occurs, (and an outbreak will occur), the team is following the same up to date documentation.

The policy is good about stating how often scanning should be done and by whom. It also mentions auditing the virus defense layers to be sure they are being implemented effectively, and who is responsible for performing that function, but does not give a time frame as to how often the audit should be done.

Summary: Overall, I would say this policy is well written and easy to understand for the intended audience. It covers most of the major areas to make it effective. It is a little bit lengthy which may make it a deterrent for the average user to take time to read. I would make the policy for GIAC a little bit less detailed but without compromising the overall message of the policy.

Also, the policy also does not give any statement as to what a consequence may be if the policy is violated. A brief statement should be included in the policy about possible actions that could be taken if an employee introduces a virus into the network that otherwise could have been prevented, because he did not follow the guidelines of the policy. Including such a statement would help GIAC with the enforcement of the policy.

Revised Policy

Title: Antivirus Policy for GIAC Wellness Enterprise
Policy No: 010
Rev: A

1.0 Purpose and Background

1.1. The purpose of this document is to outline the requirements for protection of GIAC Enterprises assets against infection by malicious code commonly known as viruses, worms and Trojan Horses. These viruses are defined as a piece of programming code usually disguised as something else that causes some unexpected and usually undesirable event. Because of the increasing number of new viruses that are introduced daily and the damage they can perform, this policy is necessary for the protection of the livelihood of this business.

2.0 Scope

2.1 This policy applies to employees, contractors, consultants, temporaries, and other workers at the Company. This policy applies to all equipment that is owned or leased by the Company or that is connected to the Company networks.

2.2 The requirements in this policy do not apply to systems that connect to Company Internet web sites and other public Internet services offered by the Company.

3.0 Policy

3.1 Certified Software

All anti-virus software utilized by GIAC will be certified by ICSA Labs.

3.2 Defense in Depth for Anti-Virus

Anti-virus defenses should follow the concept of defense in depth, deploying multiple layers of protection. Anti-virus defenses should be in place in the following areas:

A. Multi Vendor Protection: Software from multiple anti-virus vendors will be used to protect the company from viruses. Alerting: The Company should subscribe to an alerting service that warns of new emerging threats so that countermeasures can be deployed to avoid infection. These alerting services should include all anti-virus software vendors as well as a third party.

B. Internet Gateway Virus Protection**:** A server functioning as a gateway to the Internet will scan incoming traffic for viruses before the traffic reaches an internal destination.

C. Attachment Blocking**:** File types considered high risk for containing viruses will be prevented from entering the network. Information Security will maintain a list of files deemed dangerous, and will take into account the likelihood of the file type carrying a virus and the importance to the operation of the business. Files on this list should not be transferred into or out of the corporate network by any electronic means.

D. Server Virus Protection**:** Virus protection software is required on all servers connected to the Company network. Exceptions made to this policy are only allowed if it is deemed that a critical system will not function properly due to the virus software running on it. Systems in this exception should not have any programs loaded on them that commonly transfer viruses, such as electronic mail, file sharing, or web browsing. Files should not be able to be placed on these systems via drive mappings or network access. Only the IS Team manager can make the decision if a system can be placed on the exception list.

E. Desktop Systems Virus Protection**:** Virus protection software is required on all desktop computers and laptop computers that connect to the Company network. This requirement is for all systems connecting to the Company network through any connection mechanism, and it applies to company-owned assets as well as non-company-owned assets. There are no exceptions to this policy.

F. Desktop Software Virus Protection**:** Software loaded onto desktop systems should be configured to protect against viruses wherever possible. This includes but is not limited to the following:

   a) Office productivity programs should be configured to not run macros contained in documents without sufficient warning given to the user.

   b) Web browsers should be configured to block the execution of active content without the consent of the user. This includes ActiveX controls and Java applets.

   c) Electronic mail programs should be configured to guard against executing programs contained in e-mail messages. Programs in e-mail messages should never be allowed to access the user's address book or to send any e-mail messages in an automated manner.

d) All software should be updated with the latest security patches in a timely manner.

G. Antivirus Software settings: The following settings are for all systems protected with anti-virus software:

a) Anti-Virus software will be updated at least weekly with the latest definitions. Software should be updated sooner if there is a known threat.

b) All files on protected systems should be should be scanned at least once per week.

c) Automatic protection should be enabled, scanning files in real-time as they are accessed and opened.

d) All activity of anti-virus software should be logged.

4.0 Responsibility

4.1 Managers must ensure that their employees understand and comply with this policy.

4.2 Users are responsible for exercising extreme caution in order to prevent the execution of a virus.

4.3 Users must not attempt to eradicate computer viruses without expert assistance. If users suspect infection by a virus, they must immediately shut-down the involved computer, disconnect from all networks, and call for IT support.

4.4 Information Security is responsible for implementing and maintaining a layered defense strategy for the prevention of viruses.

4.5 Information Security is responsible for auditing weekly the various virus defense layers to ensure they are being implemented effectively.

4.6 Information Security is responsible for the drafting and modifying and/or updating of this policy. The GIAC management team is responsible for the review and final approval of the policy.

5.0 Action

5.1 This policy becomes effective January 1, 2003.

5.2 A procedure shall be written by IS to communicate information to users in the event of a new virus threat.

5.3 The user must play a key role in the prevention of virus outbreaks. Even though there are layers of defense technologies, an educated and cautious user is even more effective. The user is expected to:

A. Not download software without prior approval from the IS team.

B. Not use any external software other than that provide from a known and trusted provider or that which has been approved by the IS team.

C. Not intentionally generate, copy, collect, or execute any software designed to do harm to the system.

5.4 Any GIAC user who violates this policy, after having read it, will be subject to appropriate disciplinary action, which may include termination of employment, depending on the employee's intent and resulting damage by this action.

5.5 The IS team is responsible for handling any incident of virus infestation. The documented procedures are outlined in SOP 1.12 Virus Protection.

Procedure for Auditing Virus Protection on Workstations:

The Anti-virus policy listed several actions that should be carried out to ensure that GIAC has adequate protection. One of those requirements called for auditing. The following outlines the procedure for auditing the workstations at GIAC Wellness.

- What Actions should be carried out?

The purpose of this procedure is to ensure that regular audits are performed of the workstations that are used at GIAC Enterprise. All workstations that connect to the GIAC network should have the most current Norton signature file running. The Norton icon on the desktop tray should always be visible. If a user is not sure his virus protection is current or running, he should contact the GIAC desktop tech helpline.

- Why are these actions important?

The user should always exercise caution when opening email, downloading software, or sharing files as outlined in the anti-virus policy. But even the most cautious user's workstation can still become infected. Only an audit will help assist in minimizing a virus infection and perhaps show unsafe practices the user may not be aware of.

- Who is responsible for carrying out these actions?

The IS team is responsible for performing these weekly audits. A report should be generated to show a history of how well the virus protection is working on the Desktop. A good IS team should always have a way of knowing how well the defenses that are put in place are working.

- When should these actions be taken?

This procedure should be performed weekly, after the auto-scheduled weekly virus scan has completed.

The auto-scheduled weekly virus scan is run every Monday morning at 10:00 am. Users are usually logged in and connected by this time, which gives the program

the best chance of being able to scan the majority of computers that connect to the GIAC network.

- How can these actions be tested or carried out?

The IS team should perform the following procedure to audit for any viruses found:

1. Open Symantec System Center
2. Unlock the GIAC server group
3. Highlight the “Anti-virus server”
4. Sort by status
5. Highlight all machines with a status of “Virus Found!”
6. Right click > All Tasks > Logs > Virus History
7. Make note of any machines that are not responding.
8. In the Virus History window, select “Last 7 days”, then click the disk icon to export
9. Save the file to the IS secured share.
10. In the Virus History window, select “Today”
11. Sort by Action Taken
12. Write down all machines that have a virus with an action of “left alone”
13. Run a manual scan of all of the machines on the list with the following settings:
    - File types = all
    - Macro virus action 1 = clean
    - Macro virus action 2 – delete
    - Non-Macro virus action 1 = clean
    - Non-‘Macro virus action 2 = delete
    - On Advanced settings, uncheck “Show scan progress on computer being scanned” box
14. Make sure all of these scans clean or delete all of the viruses found.
15. If the same computer appears on the list for over two weeks, a desktop tech should be dispatched to the computer to have it manually cleaned.

Appendix A

The following policy for Virus protection is used at this author's company.

Title: Antivirus Policy
Policy No: 010
Rev: A

Affected Location(s):	All locations of "The Company"
Originating Dept:	Information Security
Originating Author:	IS Team Manager
Effectivity Date:	January 1, 2003

b) PURPOSE AND SCOPE

a. The purpose of this document is to outline the requirements for protection of "The Company" assets against infection by malicious code in the form of viruses, worms, and Trojan horses.

b. This policy applies to employees, contractors, consultants, temporaries, and other workers at the Company. This policy applies to all equipment that is owned or leased by the Company or that is connected to Company networks.

c. The requirements in this policy do not apply to systems that connect to Company Internet web sites and other public Internet services offered by the Company.

c) DEFINITIONS

a. Virus: A piece of programming code usually disguised as something else that causes some unexpected and usually undesirable event.

b. Worm: A self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems.

c. Trojan horse: A program that performs some unexpected or unauthorized, usually malicious, actions such as displaying messages, erasing files or formatting a disk. A Trojan horse doesn't infect other host files, thus cleaning is not necessary.

d) RESPONSIBILITIES

a. Users are responsible for exercising extreme caution in order to prevent the execution of a virus.

b. Managers must ensure that their employees understand and comply with the policy.

c. IST is responsible for implementing and maintaining a layered defense strategy for the prevention of viruses.

d. IST Information Security is responsible for auditing the various virus defense layers to ensure they are being implemented effectively.

e) POLICY

a. **Multi-Vendor Protection**
Software from multiple anti-virus vendors will be used to protect the company from viruses. The preferred method is for different vendors to be used for desktops and servers.

b. **ICSA Certification for Anti-Virus Software**
All anti-virus software will be certified by ICSA Labs.

c. **Anti-Virus Software Settings**
The following settings are for all systems protected with anti-virus software:

i. Anti-Virus software will be updated at least weekly with the latest definitions. Software should be updated sooner if there is a known threat.

ii. All files on protected systems should be should be scanned at least once per week.

iii. Automatic protection should be enabled, scanning files in real-time as they are accessed and opened.

iv. All activity of anti-virus software should be logged.

d. **Alerting**
The Company should subscribe to alerting services that warn of new emerging threats so that countermeasures can be deployed to avoid infection. These alerting services should include all anti-virus software vendors as well as a third party.

e. **Defense in Depth for Anti-Virus**
Anti-virus defenses should follow the concept of defense in depth, deploying multiple layers of protection. Anti-virus defenses should be in place in the following areas:

i. **Internet Gateway Virus Protection**
A server functioning as a gateway to the Internet will scan incoming traffic for viruses before the traffic reaches an internal destination. Gateway servers include but are not limited to e-mail servers and proxy servers.

ii. Attachment Blocking
File types considered high risk for containing viruses will be prevented from entering the network. Information Security will maintain a list of files deemed dangerous, and will take into account the likelihood of the file type carrying a virus and the importance to the operation of the business. Files on this list should not be transferred into our out of the corporate network by any electronic means, including but not limited to electronic mail, FTP, and HTTP.

iii. **Server Virus Protection**
Virus protection software is required on all servers connected to the Company network. Exceptions to this policy are made in the following situations:

1. If it is determined that running virus protection on a critical system will cause undue system load or system instability,

and that the system is not at unreasonable risk of being infected with a virus, virus protection software is not required. Systems in this exception category should not have any programs loaded on them that commonly transfer viruses, such as electronic mail, file sharing, or web browsing. Users should not be able to place files on these systems through drive mappings or other network access.

2. When virus protection interferes with lab testing, the lab server should have virus protection software installed and the entire systems scanned to ensure a clean system. Once a clean system is ensured, virus protection software can be disabled for the duration of the test. While the software is disabled, No programs should be run that commonly transfer viruses, such as file sharing or electronic mail. Once the testing is complete, the virus protection software should be enabled.

iv. **Desktop Systems Virus Protection**
Virus protection software is required on all desktop computers and laptop computers that connect to the Company network. This requirement is for all systems connecting to the Company network through any connection mechanism, and it applies to company-owned assets as well as non-company-owned assets. There are no exceptions to this policy.

v. **Desktop Software Virus Protection**
Software loaded onto desktop systems should be configured to protect against viruses wherever possible. This includes but is not limited to the following:

1. Office productivity programs should be configured to not run macros contained in documents without sufficient warning given to the user.

2. Web browsers should be configured to block the execution of active content without the consent of the user. This includes ActiveX controls and Java applets.

3. Electronic mail programs should be configured to guard against executing programs contained in e-mail messages. Programs in e-mail messages should never be allowed to access the user's address book or to send any e-mail messages in an automated manner.

4. All software should be updated with the latest security patches in a timely manner.

vi. **User Awareness & Responsibilities**
The user must play a key role in preventing virus outbreaks. Even though there are layers of defense technologies, there is nothing more effective in the prevention of viruses than an educated and cautious user.

1. **Users Must Not Attempt To Eradicate Computer Viruses**
   Because viruses have become very complex, users must not attempt to eradicate them without expert assistance. If users suspect infection by a virus, they must immediately shut-down the involved computer, disconnect from all networks, and call the Helpdesk.

2. **Prohibition Against Downloading Software From Third Party Systems**
   Users must not down-load software from dial-up electronic bulletin board systems, the Internet, or any other system outside the Company without the prior approval of IST.

3. **Testing For Viruses Prior To Use On Company Systems**
   To prevent infection by computer viruses, users must not use any externally-provided software from a person or organization other than a known and trusted supplier. The only exception to this is when such software has first been tested and approved by IST.

4. **All User Involvement With Computer Viruses Prohibited**
   Users must not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of or access to any Company computer, network, or information.

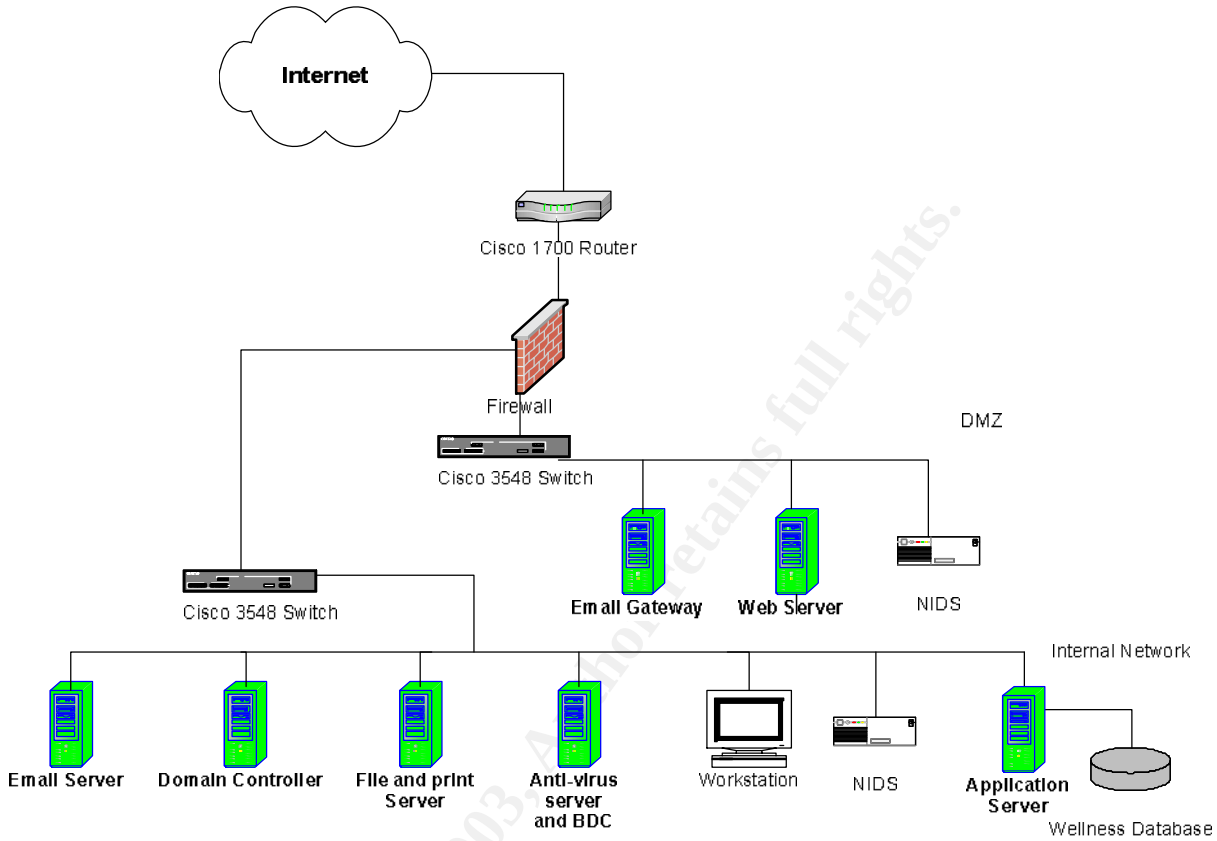
5. **Communication to Users**
   A procedure should be written to communicate information to users in the event of a new virus threat.

6. **Virus Hoaxes and Warnings**
   Users should not spread any virus warnings they receive from outside sources to other users in the company. The vast majority of these warnings are hoaxes, and the resulting scare often does more damage than a virus itself. If a user receives a virus warning, the Helpdesk should be notified immediately.

vii. Incident Response

The Company will have a virus emergency response team prepared to deal with a virus infestation should one occur. The team will follow documented procedures for analyzing the situation, minimizing the damage, and eradicating the virus.

Figure 1



References

Joel Deitch – Editor in Chief: “Dynamic Threat Protection”, February 2003, ISS Connect Magazine.

Howard A. Schmidt: “Strategic Thinking”, 2002 CISO Magazine.

Jayne Parkhouse: “Riding the Storm”, July 2002, SC Info Security Magazine.