Global Information Assurance Certification Paper

The GIAC Group

By: Gregory S. Roy

GIAC Information Security Officer (GISO) Certification
Practical Assignment: Version 1.3 (February 7, 2003)

The GIAC Group
Table of Contents

Abstract

The purpose of this practical is to demonstrate the understanding of course materials for participants who attended the SANS Information Security Officer Training and whom are studying for their GISO certification. A fictional company will be described along with its business operations and information technology (IT) infrastructure. Three security risks will be identified and explained. Steps on how to mitigate the three risks will be provided. An existing security policy will be analyzed and discussed in detail. A revised security policy will be implemented and a procedure written to enforce the updated policy.

Assignment #1 – Describe The GIAC Group

The GIAC Group Description

The GIAC Group is a medium-sized privately owned business of 3000 employees dedicated in providing various security services to private companies and government agencies. The company provides security assessments and prepares security policies for its customers. It has one main office located on one floor of a single building in a secure industrial complex in Kansas City, MO. Most of its employees are disbursed across the country near most major cities and they obtain all correspondence and assignments remotely by accessing the company's computers from home or a client site using a dial-up communications server. The GIAC Group has complete disaster recovery and business continuity plans and procedures in place. It has a contracted warm-site in Atlanta, GA, which can be brought up in 24 hours after a disaster so full business operations can resume. The company's infrastructure and business model enable it to respond immediately to proposals for it contracting services. Little travel is required of employees and there is high employee morale. There is a low total cost of ownership in implementing new employees.

The GIAC Group IT Infrastructure

This section describes the IT infrastructure of The GIAC Group. See Appendix A for the current infrastructure diagram.

Employees access the corporate LAN through modems on their workstations or laptops and dial-in through the public switched telephone network (PSTN) through a Remote Access Server (RAS). The internal network of The GIAC Group is used to store client data received by its employees and to process internal applications required to support its core business functions. Clients access a read-only public web server containing information about The GIAC Group, the services it provides to clients, various security and policy information, and company contact information. All traffic from the Internet is filtered through a Cisco router, a Checkpoint firewall, and a switch in the Demilitarized Zone (DMZ). Its public web server, email gateway, and File Transfer Protocol (FTP) server all reside in the DMZ. Intrusion detection systems (IDS) are found both in

the internal and external networks. An IBM mainframe resides in the internal network and houses separate databases for its financial and client data. An email server, anti-virus server, file/print servers, and corporate workstations round out the internal network.

Elevators that operate during normal business hours control physical access to the corporate office. Employees obtain access to the stairwell leading to the office during off-duty hours with a coded ID badge that provides access. A receptionist controls the access of visitors, all must sign in and out. The web and data servers are located in a controlled access room with monitored video cameras. Only authorized members of the IT staffs are granted access with their ID badge. The ID badges also permit controlled access to various management offices.

- All employees' use certified Compaq workstation/laptops running Windows 2000 Professional, SP3. All are configured with standard ZENworks images for the operating system with all service packs and security fixes, Microsoft Office 2000, Internet Explorer 5.5, RUMBA mainframe emulation, and Norton Antivirus Corporate Edition, and other miscellaneous software, etc. All external workstations/laptops have 56K, V.92 modems in order to access The GIAC Group remotely. No internal workstations have installed modems. All have network connectivity and Internet access and access is currently not routed through a proxy server.

- The Remote Access Server is a Cisco AS5300. Employees dial either a local or 1-800 number for access. The RAS is currently configured as a PPP type server using the TCP/IP transport. Authentication is by username/password and never expires. The current policy allows more than three logon attempts.

- The switches are Cisco Catalyst 3550 Series Intelligent switches. It is used to provide private IP addressing throughout the DMZ and internal local area network (LAN).

- The high capacity Cisco router is a 7500 series and it routes all incoming/outgoing traffic from the Internet and the DMZ. The router can deny unauthorized traffic by shutting down restricted ports.

- The firewall is a Checkpoint 4.1 NAT. All Internet traffic is routed through the firewall. It has been configured, according to policy, to deny by default. All traffic not allowed is blocked.

- The network intrusion detection (IDS) runs Symantec Host IDS 4.1 to monitor traffic patterns and perform packet logging and reporting of unauthorized activity in the DMZ and internal network.

- The IBM mainframe the latest version of z/OS and maintain the corporate DB2 databases of financial and client data.

- The internal email server is Microsoft Outlook and the file and print servers handle the storage of corporate files on the LAN and printing duties. The anti-virus server handles the distribution of patches, virus pattern updates, and virus notification centrally. The internal Domain Name System (DNS) handles the translations of domain names and IP address.

- The servers in the DMZ are all Compaq servers running Windows 2000 Server with all service packs and security fixes applied. McAfee Anti-Virus Server Editions run on all the servers. The servers are configured and hardened using industry standard checklists for all installed software before deployment. There is currently no content filtering.

- The public web server in the DMZ is for the general public, the prospective clients, and current clients. This is where to go to find out more about The GIAC Group, the services it provides, security and policy information, contact information and restricted access to client's own data.

- The FTP server in the DMZ currently only used to propagate the data on the public web server from the internal network. Access to the server is blocked on port 80 as the data is propagated.

Note: There are known deficiencies in the currently infrastructure and they are currently being addressed. The GIAC Group grew fast for a company its size and spent most of its time focusing on its business model.

The GIAC Group Business Operations

The GIAC Group receives a portion of its business through a government issued business process agreement (BPA) and the remaining portion through word of mouth, targeted emails, and from requests generated from its public web site. In the last few years, security has become the top priority at most private companies and government agencies.

In-house at the company's office in Kansas City, MO, enough personnel is available to support the mainframe environment, the local area network (LAN), the databases, all servers, and the rest of the telecommunications and information resources infrastructure. There is a staff for office operations for human resources, security, and a staff to support the operation and maintenance of all software.

The IT Resources Office follows a documented backup and recovery process and a full backup of all file and databases are performed daily inside the internal network. The data on servers in the DMZ have full backups performed twice a

week and incremental backups in between. Two copies are made of full backups, one is keep in-house and the other is sent off site for more secure storage. In the event of a serious disaster, the storage vendor can immediately provide backup tape at the company's disaster recovery site.

The hiring of new remote employees is done for the most part electronically. The public web server hosts an Employment area and contains the requirements for working for The GIAC Group, applications to fill out for employment, and an email address to forward employment correspondence. Candidates are interviewed and proof of their credentials must be provided. If a candidate is selected for employment, they are emailed an employee orientation packet. The packet includes forms that must be filled out and returned. It includes payroll, w-2, health insurance, life insurance forms, etc. Also included are forms for non-disclosure agreements. The packet also has an employee handbook covering all policies and regulations they are required to follow as well as the information necessary to access the corporate network through the RAS. Remote employees are required to access the corporate network using their own workstation or laptop. The software for employee jobs can be either downloaded or requested through email for an employee installation CD that is sent federal express (FEDEX).

Remote employees must log in through the remote access server (RAS) in order to send/receive corporate email, access the LAN, and to access and provide data about clients in the database.

Prospective clients usually respond to the targeted emails. The emails include an electronic brochure with information about The GIAC Group. It includes a description of "who we are" and "what services we provide." Because the company provides security assessments and prepares security policies for its clients, the brochure explains in detail the reasons for security assessments and security policies. Included is a link to the public web site and a specific email address.

Other prospective clients, by word of mouth, obtain the email address and link to the public web site from our current clients. The information provided in the electronic brochure is also available on the public web site. The prospective clients respond to the specific email address indicating which client referred then to The GIAC Group. They are then sent the electronic brochure.

The specific email address is strictly monitored and a response is guaranteed within 2 hours. Interested clients produce a statement of work (SOW) listing which services they are requesting and the location of the request. Governmental clients also issue a SOW through the BPA. In both cases, The GIAC Group then provides through email, a technical proposal that the client must either accept or reject. The GIAC Group lists the services they will be providing in the proposal as well as a breakdown of the costs. If the proposal is

accepted, paperwork is signed binding the contract, and all other necessary forms such as non-disclosure agreements, etc. A remote employee is immediately assigned to the client in the designated city as listed in the SOW and is guaranteed to be on-site by the next business day. The GIAC Group employee will lead a kick-off meeting to discuss the company methodology and give an overview of what The GIAC Group expects of the clients. Interviews are conducted at the client's site and documentation is gathered. Soft-copy documentation is preferred. The employee assigned to the client analyzes and prepares his reports and logs in through the RAS to upload data to the LAN. An in-house analyst then reviews the client data again and it is loaded into the client database. Formal reports are then produced. Copies are emailed to the assigned employee and client for review and revision, if necessary. Final copies are distributed in the same manner.

The one thing that is most important to the success of The GIAC Group is the confidentiality, integrity, and availability of our client's data. Sensitive information is captured about a client's computing infrastructure, physical security, technical, operational, and management controls. This data in the client database represents one its "crown jewels." Even though a policy of least privileged access has been instituted against the database, it's not enough. The second most important are our remote employees. Analyst handle sensitive information about our clients, sensitive corporate methodologies about security, and employee/client email addresses. The company's infrastructure enables it to quickly respond to clients also gives it a business edge on its' competitors.

Assignment #2 -- Identify Areas of Risks

A thorough analysis of The GIAC Groups' IT infrastructure and business operations have identified three critical security risks. Risk is often defined as the potential for loss or harm as the result of a threat combined with a particular vulnerability.

Area of Risk #1 **:** Remote access to The GIAC Group's corporate network allows potential unauthorized access to its "crown jewels", sensitive data about its clients and corporate data.

The GIAC Group's remote employees access the corporate network by dialing in through the Remote Access Server (RAS). The employees send and receive email, access the LAN, and access data in the databases. The RAS is un-secure. User authentication is by a static username and password. Dial back authentication is not performed. It allows an undetermined number of logon attempts and no time restrictions imposed on the employees. The RAS is directly connected to the corporate internal network and there is no firewall between the RAS and the internal network. There is no implemented remote access policy.

Sensitive data about client's IT infrastructure, physical security, various security controls flows through the RAS and The GIAC Group's internal network. Potential exists for a hacker to spoof one of our remote employees, circumvent our RAS security controls, and possibly gain access to the company's internal network. The use of "war dialers" by hackers or unauthorized users would allow it to obtain a valid dial-up access number and eventually guess employees' ids and passwords. Since there are no time restrictions on remote users and limits in the number of logon attempts, armed with sophisticated software tools, these hacker or unauthorized users would assume the identity of an authorized remote employee. After successfully penetrating the internal network undetected, they could install key-loggers and other spy tools to obtain further access to exploit other known vulnerabilities to systems and application within the network. These intruders could obtain access to The GIAC Group's financial and client database and possibly corrupt the data. This is considered a critical risk. If the client's security controls and infrastructure were obtained, they would be exploited as well. If The GIAC Group were compromised and its "crown jewels" obtained, just by one incident, the resulting consequences would be catastrophic. The embarrassment, lost customer confidence, loss of company assets, and irreparable harm would be substantial for The GIAC Group and its clients. Its reputation would be ruined, clients lost, loss of revenue, and it would become entangled in legal litigation.

Steps to mitigate the risk:

- Configure the software on the RAS to disconnect modems for a set period time of period if the allotted number of dial-in attempts is exceeded per industry standards. For example, disconnect modems for 15 minutes if number of dial-in attempts exceeds three (3). Allow modem access only during core business hours.
- Analyze access logs on a regular basis for irregular activity, especially failed attempts.
- Allow remote employee to set own password and force reset every month. Implement a second password for more protection in the event the first password is compromised.
- Remove access to employees when not needed, immediately upon retirement or termination. Apply the concept of least privilege.
- Impose time restrictions on remote access.
- Develop and implement a remote access policy defining the standards and procedures for access to The GIAC Group. A policy would minimize the potential exposure of The GIAC Group to damages resulting from the unauthorized use of company resources and the protection of its "crown jewels".

Area of Risk #2: Remote employee workstations and laptops are not updated with the latest security patches and software upgrades.

The GIAC Group's remote employees access use their own workstation or laptop to access the corporate network by dialing in through the Remote Access Server (RAS). When a remote employee is hired, a request is submitted for installation software on CD to install the same software and security patches as the workstations in the corporate office. The workstations in the corporate office are configured with the same software images using ZENworks, so all software and patches are kept current. All updates are pushed to each internal employee's workstation upon network logon. The GIAC Groups' IT Resources Office have indicated the biggest vulnerability is the inability to manage and apply security patches to remote employee workstations and laptops. There is inadequate control of software distribution and patches, especially security patches. Application security features and other security controls are incorrectly configured and maintained. No software auditing is done. There is possible use of unauthorized software.

There is no specific security policy and procedure at The GIAC Group ensuring software and security patches are applied to remote employee computers. This poses a significant risk to The GIAC Group. The un-patched remote workstations and laptops expose the company to a wide range of vulnerabilities both externally and internally. The news media reports daily of exploited vulnerabilities. Vulnerabilities such as the a buffer overruns in Microsoft Internet Explorer, certificates in Microsoft Exchange server lead to information disclosure, and default Microsoft Windows 2000 permissions could allow Trojan horse program are some examples. The Microsoft Security Bulletin MS02-064 gives a technical description of this last vulnerability:

> On Windows 2000, the default permissions provide the Everyone group with Full access on the system root folder. In most cases, the system root is not in the search path. However, under certain conditions – for instance, during logon or when applications are invoked directly from the Windows desktop via Start | Run – it can be. This situation gives rise to a scenario that could enable an attacker to mount a Trojan horse attack against other users of the same system, by creating a program in the system root with the same name as some commonly used program, then waiting for another user to subsequently log onto the system and invoke the program. The Trojan horse program would execute with the user's own privileges, thereby enabling it to take any action that the user could take.[3]

This vulnerability exemplifies the need to keep systems patched. Also, the remote users can download un-authorized software and expose the company to a workstation or laptop tainted with spyware, malware, adware, key-loggers, data miner cookies and more. Why is the IT staff concerned? A lot of the threats to The GIAC Group network might not detectable by the existing security tools and controls. Even with the tools and controls in place, the network might still be compromised. Remote employee ids and passwords could be stolen, sensitive

client data about its IT infrastructure, physical network, and security controls, and sensitive corporate methodologies and other intellectual property could be obtained by hackers and these tools to phone home the "crown jewels."

Steps to mitigate the risk:

- Develop and implement a policy and/or procedure to complement the remote access policy defining the standards and procedures for software installation and maintenance.
- Pre-configure laptop with all required software and patches and send laptop to new remote employees.
- Install either the Microsoft Baseline Security Analyzer or CIS Scoring Tools on each workstation and remote laptop to identify uninstalled security patches and report back to the IT Resources Office.
- Push any software changes and patches to employee computers through an automated software distribution product upon network logon.

Area of Risk #3: The Security Awareness Program is outdated.

All The GIAC Group's employees receive an employee orientation packet upon hire. The packet includes a copy each policy and regulation all employees must adhere to. The GIAC' Groups Acceptable Use Policy must be read and an electronic acknowledgement returned to the corporate office by email before the distribution of a user id and password. The employee installation CD contains a Security Awareness Training module. Upon completion of the training, a completion form is also emailed to the corporate office. The GIAC Group's Security Officers have discovered many risks. The Security Awareness Training is insufficient and incomplete. Training is performed only upon hire and annually. There are no auditing controls ensuring employees actually completed the security training. There is a total lack of user awareness on behalf of most employees, especially remote employees, on the use of passwords. Employees have been susceptible to eavesdropping, masquerading, and social engineering, and they are not aware enough about the all the risks associated with software viruses.

The GIAC Group's Management and Security Officers are very concerned. "Studies show that a company's biggest security threat is its own employees."[4] The company's remote employees interact daily with clients, usually at the client's office. Most of The GIAC Group's internal employees interact with clients, salesmen, and contractors, etc. The nature of the business makes its employees vulnerable to social engineering and masquerading. User ids, passwords, email addresses, and important points of contact can be obtained by hackers and others by eavesdropping on telephone conversations or by "shoulder surfing" while email is read. Unsecured sensitive documents that are not locked up, left unattended, or not shred before disposal can be obtained

easily. Armed with the right information, an employee's identity could be falsified by a perpetrator. For instance, a call can be made to the Help Desk and a request be made to reset a password for a dial-up id. Since the id is known and the password is reset, a perpetrator has almost been guaranteed access to the corporate network. If a dialup number is discovered, they are in, undetected. Sensitive client and corporate data can be compromised.

Steps to mitigate the risk:

- Test employees on Security Awareness on regular basis, every 3 months to coincide with password policies. Ensure that the security basics are covered including physical security and disaster recovery.
- Provide customized Security Awareness training depending upon the job title or function. Ensure course completion by auditing.
- Incorporate security tips in screen savers or log-on banners for all employees. Incorporate tips such as lock or logoff your screen when leaving your desk unattended and scan all email attachments for viruses before opening.
- Display Security Awareness Banners throughout the corporate office in visible areas. Deliver Security Awareness pamphlets and reminders through email. Distribute trinkets with security tips printed on them, such as pens and notepads.

Assignment #3 – Evaluate and Develop Security Policy

Evaluate Security Policy

The GIAC Group noted the lack of a Remote Access Policy. A Remote Access Policy was taken from the SANS Security Policy Project. The full un-altered policy is included in the Appendix with the proper reference.

Purpose:

The policy's purpose statement is very clear, concise, and to the point. It's easy to determine why the policy was written. It provides for emerging types of future host connectivity. In the future, employees will have the capability to use other devices such as cell phones, kiosks, etc. to connect to the company network.

Background/Scope:

This statement clearly states whom the policy applies to. The listed parties are the only ones who should legitimately have remote access to the network. It's a little perplexing why the statement, "including reading or sending email and viewing intranet connections", was included as written. It's one of the fundamental reasons for remote access. You should either leave the statement off or add more examples so the readers understand the other corporate resources available for remote access. It can go either way and is a matter of interpretation. Not all acronyms are listed in the Definitions, SSH is missing.

Policy Statement:
This section is the most confusing, unclear, and possibly incomplete of the whole remote access policy. The use of the phrase "same consideration" is not clear. It can be used in too many contexts. The entire section under 3.1 General, number 2, should be removed entirely. The information is false and inaccurate but should reside in an Acceptable Use Policy. I would re-write this portion of the policy for clarity and place it in the Acceptable Use Policy. This policy references other polices because of the similar requirements of each policy. The policies required are different for each company, depending on its infrastructure and business model. If a policy is nearly similar, combine them into one policy. Too many included references to other policies leads to confusion and employees would be unlikely to read all of them. The last section under 3.1 General, number 4, is also unclear. A company may have a website with the information, but it sounds more like information found on an Internet Service Provider (ISP) site. The information available could be misinterpreted. Is the website internal or external? It should reside on the intranet. Putting information on a website on how to connect to your internal website would be a risk in itself.

All is reasonably clear under the requirements portion of the policy. Reference is made the company's Password Policy where employees can review the standards for creating, protecting, changing passwords. Without this policy for guidance, the corporate network is susceptible to compromise. Very good requirements are listed: do not share your logon and email passwords, do not connect to the corporate network and another network at the same time, and don't mix official and personal business when remotely access the network. There is a requirement stating non-standard remote access configurations need approval, but it's not a good idea to support too many configurations. The direction for remote access with its policies and configurations should originate from within the organization and not from the employees. The IT Security and Resources Office should jointly determine remote access methods.

Responsibility:
No one has been designated a responsible party for any parts of the policy. The policy is ineffective and un-enforceable. There needs to be designated employees responsible for writing it, reviewing it, approving it, modifying it, and someone for the implementation of it.

Action:
The policy does indicate some of the specific actions required in order to comply with the Remote Access Policy. One major problem is lack of compliance dates or timelines. Coupled with no designated responsible parties for enforcement, we have an ineffective policy. Any policy changes, either minor or major, need specific dates listed on when the changes take effect and when compliance is expected by the governing body on the IT Security Office. The GIAC Group cannot mitigate the risks associated with remote access by this policy as listed.

Summary:
As a whole, I would say this policy is well written, clear, and easy to understand on most of its points. There are some ambiguities that need addressing. The intended audience of the policy is identified, but I feel it elaborates too much on family member access. I would eliminate the references to inapplicable polices and terminology as it applies to The GIAC Group. I would combine similar policies, such as remote access and VPN, because they are nearly similar and meet the GIAC Group's requirements. The employees won't read all the policies if they have to sift through too many to obtain enough information on remote access. As stated above, the policy needs designated responsible parties. I would make the policy a little more detailed to conform to The GIAC Group. The GIAC Group cannot mitigate the risks associated with remote access by this policy. Because of The GIAC Group's infrastructure whereby most of its employees are external, increased resource requests, and the non-existence of an applicable policy, a remote access policy should be created to define permitted remote access and resources. Changes are necessary in the policy and possibly in its IT infrastructure.

Revise Security Policy

Note: Appendix C contains the revised Infrastructure Diagram for The GIAC Group conforming to the new remote access policy.

Remote Access Policy
The GIAC Group

To: All Employees of The GIAC Group
Date: June 26, 2003

1.0 Purpose:
The purpose of this policy is to define standards for connecting to The GIAC Group network from any host outside the corporate internal network. These standards are designed to minimize the potential exposure to The GIAC Group from damages, which may result from unauthorized use of The GIAC Group resources. Damages include the loss of sensitive confidential data about client's IT infrastructure, physical security, and security controls, company confidential data and intellectual property, damage to public image, risk of legal litigation, damage to critical The GIAC Group internal systems, etc.

2.0 Scope:
This policy applies to all The GIAC Group employees with a The GIAC Group-owned laptops or workstations used to connect to The GIAC Group network. This policy applies to remote access connections used to do work on behalf of The GIAC Group. Some examples of remote access connections permitted are

corporate email, web based applications, client server applications, LAN resources, etc.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, DSL, SSL VPN, SSH, and cable modems, etc.

3.0 Required Policy Actions:

1. A SSL VPN is the required remote access connectivity method for The GIAC Group corporate network.
2. All employees will be required to request an SSL VPN account through their Division Supervisor. The request is forwarded to the IT Security Office for final approval pending background checks. After approval the IT Resources Office is notified to configure a laptop for immediate shipment to the employee.
3. Employees are responsible for selecting a high-speed ISP to coordinate the installation of any required hardware and software and the payment of access fees.
4. Additional information regarding The GIAC Group's remote access connectivity method is available through the IT Security Office. It is the responsibility of The GIAC Group employees with SSL VPN account to ensure that unauthorized users are not allowed to access to The GIAC Group internal network.
5. The SSL VPN account must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. Refer to the Password Policy for additional information on the creation of strong pass-phrases.
6. Each employee agrees to use the SSL VPN account for official business only.
7. Employees that are actively connected to The GIAC Group network are not permitted connections to any other network. All other traffic will be denied by default.
8. Dual split-tunneling or dual homing is not permitted at any time.
9. One network connection is allowed and employees will be automatically disconnected from The GIAC Group network after fifteen minutes of inactivity. Employees must logon again to reconnect to the network.
10. The GIAC Group's IT Resources Office will configure all laptops for remote access. All software will be configured with the standard ZENwork images including all virus updates, service packs, and security patches.
11. All hosts that are connected to The GIAC Group internal networks via the SSL VPN account must use the most up-to-date anti-virus software as specified in the company Anti-Virus policy.
12. The use of Peer-to-Peer (P2P) networks is strictly prohibited as specified in the company Acceptable Use policy.

4.0 Enforcement:
Any employee found to have violated this policy may be subject to disciplinary action, with penalties ranging from reprimand up to and including termination of employment.

5.0 Designated Responsibilities:
5.1 Employee -- Ensure that unauthorized users are not allowed to access to The GIAC Group internal network. Select their choice of high-speed ISP, either cable or DSL, and abide by all policies and procedures of The GIAC Group.

5.2 Division Supervisor – Requests SSL VPN account on employee's behalf and forwards requests to the IT Security Office. Verify legitimacy for access. Reviews policies and assists in the approval process.

5.3 IT Security Office – Reviews, develops and maintains all security policies and procedures for The GIAC Group. Receives all SSL VPN remote access requests from the Division Supervisors. Perform all background checks on employees before granting access to company resources. Maintain final approval on all requests. Forwards SSL VPN remote access requests to the IT Resources Office for laptop configuration. Determine disciplinary actions for policy violations and recommend termination of employment, if necessary.

5.4 IT Resources Office – Receives SSL VPN remote access request from the IT Security Office. Configures all laptops for remote access. All software is configured with the standard ZENworks images including all virus updates, service packs, and security patches. Duties also include all software on internal employee workstations. It handles shipping of laptops to the remote employees.

5.5 IT Network Office – The GIAC Group's network infrastructure support team whose responsibility is to update and maintain the entire network infrastructure according to all security requirements, policies and procedures.

6.0 Compliance Date:
This policy takes effect on October 1, 2003 and compliance is mandatory. This policy replaces the company's Dial-In access policy.

Personally-owned computers or workstations will be allowed to continue assessing the corporate network only until this policy takes effect.

7.0 Definitions:

Term	Definition
Cable Modem	Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.

Dial-in Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a The GIAC Group-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into The GIAC Group and an ISP, depending on packet destination.
DSL	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
Peer-to-Peer	“Peer-to-peer (P2P) is a type of transient Internet network that allows a group of computer users with the same networking program to connect with each other and directly access files from one another's hard drives.”[2]
Proxy	A firewall mechanism that replaces the IP address of the host on the internal protected network with its own IP address for all traffic passing through it. A intelligent software agent that authenticates the client IP address.
Remote Access	Any access to The GIAC Group's corporate network through a non-The GIAC Group controlled network, device, or medium.
Split-tunneling	Simultaneous direct access to a non-The GIAC Group network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into The GIAC Group's corporate

	network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.
SSH	Secure Shell, a completely encrypted connection between two machines protected by a super long pass-phrase.
SSL VPN	A Virtual Private Network that "uses SSL and proxies to provide authorized and secure clientless to HTTP, client/server, and file sharing resources. Combining proxy technology with SSL prevents users from making a direct connection into a secured network and provides granular access control by user, group, application, or URL. This ensures only authorized users have access to the resources allowed by the company's security policy."[5]
VPN	A protocol for establishing private communications over a public network.

8.0 Revision History:
Version 1.0 created June 19, 2003. Annual review is scheduled one year past implementation date.

Assignment #4 -- Develop Security Procedures

Remote Access Procedures
Laptop Configuration for Remote Access
The GIAC Group

Purpose:
The purpose of this procedure is to define the steps required by the IT Resources Office in configuring laptops for remote access. This procedure is used to supplement the implementation and enforcement of the overall The GIAC Group Remote Access Policy.

- What actions are carried out?

Define the steps required to configure laptops for external employees for remote access to The GIAC Group corporate network using a clientless SSL VPN account. The IT Resources Office must configure all laptops for remote access internally. Novell's ZENworks is used to create images of all software used including, virus updates, service packs, security patches, security policies, and spyware tools, etc.

- Why are the actions important?

By keeping control of the software installation under a central group, all software and patches can be thoroughly tested before being deployed to all employees. Employees automatically receive all required updates upon next logon to the corporate network. The risks associated with remote access can be mitigated to the lowest acceptable levels.

- Who bears the responsibility for the execution of the actions?

The IT Resources Office bears the responsibility for configuration of the laptops for remote access. An employee's Division Supervisor initiates the request. Different employees are given access to applications based on the principle of least privilege. Some have access to the client database, some to the financial database, and other just have access to the Microsoft Office applications and corporate email, etc. The IT Security Office receives the request and references an application access matrix to determine the employee's access level. A unique digital certificate is created and is sent with the approval documentation to the IT Resources Office and is configured on the laptop.

- When and/or where should the actions be taken?

The procedure to configure laptops for remote access is performed daily until all remote employees have requested and received laptops for remote access. The procedure will be performed as requested after the policy's compliance date takes effect.

- How are the actions tested or verified?

The IT Resources Office performs the following procedure when configuring laptops for remote access:

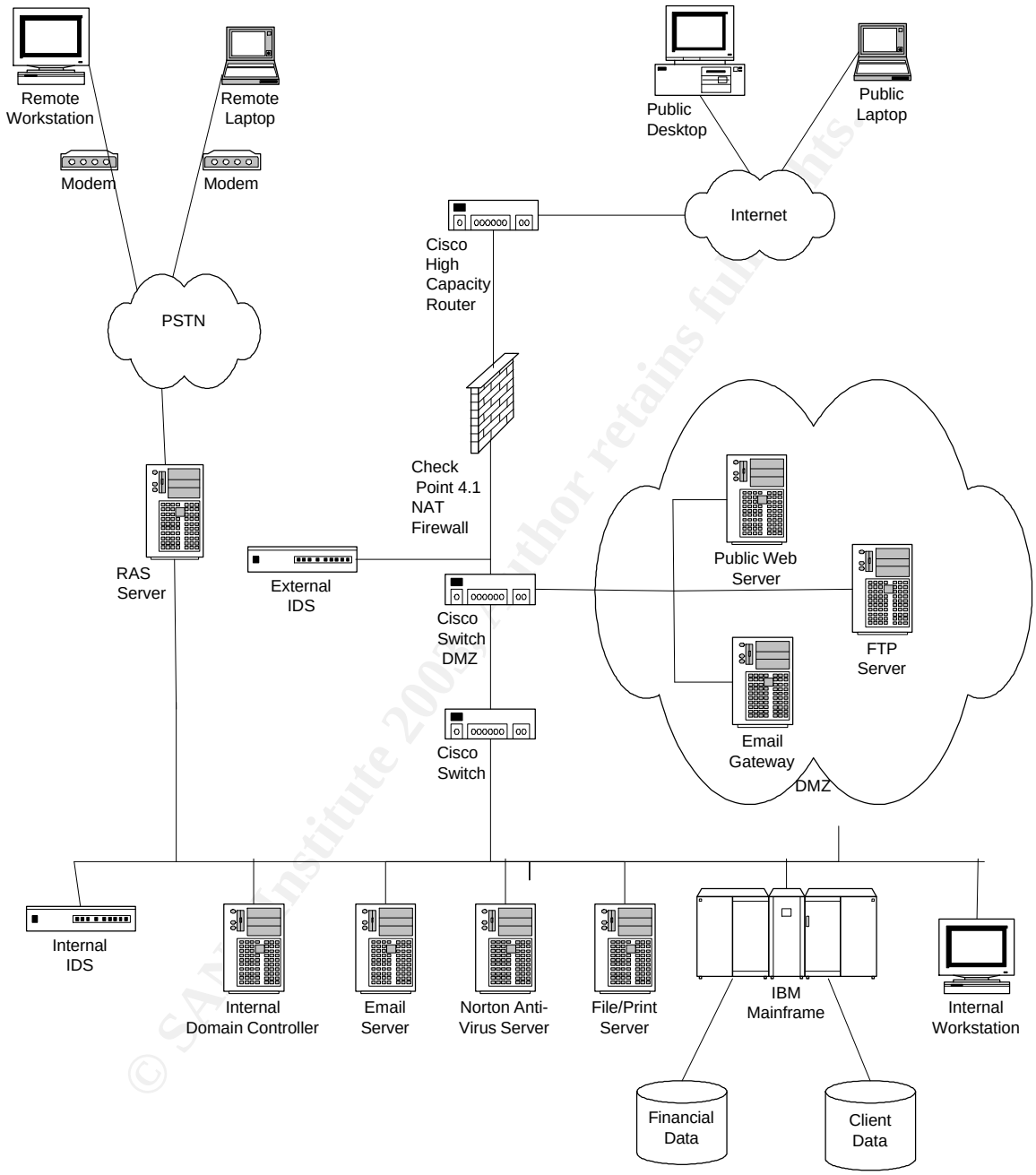
1. Receives security request form from the IT Security Office with the attached application access matrix and digital certificate.
2. Acknowledges receipt of the request and notifies the employee, Division Supervisor, and IT Security Office that the request is in progress.
3. Checks out a new laptop and reformats the hard drive.
4. Use ZENworks to push Windows 2000 Professional, service packs, and security patches images onto laptop.
5. Use ZENworks to push Microsoft Office Suite, service pack, and security patches images onto the laptop.
6. Use ZENworks to push RUMBA, Norton Antivirus Corporate Edition, and remaining miscellaneous software images onto the laptop.
7. Use ZENworks to push PestPatrol Corporate Edition onto the laptop. "The following options are configured for maximum spyware and computer pest removal:
    - Go to the Options | Automatic scans tab.
    - Scan on Boot, not checked.
    - Invoke on Boot, default.
    - PPControl, places icon in systray.

    - Cookie Control, set to delete all spyware cookies automatically.
    - KeyPatrol, default to identify keyloggers."[8]
    - Set Task Scheduler to execute daily at noon.
8. Use ZENworks to push ZoneAlarm Pro onto the laptop. Firewall is disabled until high-speed ISP is installed and configured.
9. Follow steps listed in the "Windows 2000 Professional Baseline Security Checklist"[6] specifically:
    - Set logon message title and text for users attempting to log on, indicating that users must have proper authorization to logon and urge them to disconnect immediately if not authorized, etc.
10. Use ZENworks to push Microsoft Baseline Security Analyzer[7] image onto the laptop. The following options are preset as follows:
    - Select "Scan a computer".
    - Select options to check for Windows vulnerabilities, weak passwords, and security updates.
    - Select option for "Use SUS Server" and input its name to perform the security updates check against the local internal SUS server.
    - Set Task Scheduler to execute weekly upon initial network logon.
    - Report emailed back to corporate office.
11. Apply appropriate Windows 2000 security policy and load digital certificate
12. Package and ship laptop Federal Express to the employee. Included are setup instructions.
13. Marks security request as shipped but not received and notifies the employee, Division Supervisor, and IT Security Office of shipment and provides the tracking number.
14. The IT Resources Office monitors the tracking number to ensure delivery.
15. Employee acknowledges receipt of laptop to Division Supervisor, IT Security Office, and IT Resources Office.
16. Employee is emailed password from the IT Security Office.
17. Employee connects to high-speed ISP and authenticates against the SSL VPN with the emailed password. The digital certificate is activated. The employee accesses all approved resources.
18. Use corporate network logon id/password to access network. Installation and configuration is not complete until logon is successful. Any application updates, virus updates, service packs, and security patches are pushed to laptop through ZENworks if necessary upon each network logon.
19. The Division Supervisor, IT Security Office, and the IT Resources Office receives email notification from employee that laptop is configured and complete.
20. The IT Resources Office marks the security request complete and notifies all parties.
21. The Microsoft Baseline Security Analyzer Tool runs weekly and emails the reports back to the IT Resources Office. The reports are analyzed and if new vulnerabilities are detected, the patches are downloaded. The

appropriate software image is rebuilt, tested, and pushed out to the remote laptops.

22. PestPatrol Corporate Edition tool runs daily at noon and detects and eliminates Trojan horses, Hacker Tools, and Spyware/Adware such as data mining or tracking cookies from employee laptops.
23. Employees are restricted from installing any software, including downloads from the Internet, and is controlled by security policy.

Appendix A
The GIAC Group Infrastructure Diagram
Current



Appendix B
Sample Remote Access Policy

This policy was obtained from the SANS Security Policy Project[1].

Remote Access Policy

1.0 Purpose
The purpose of this policy is to define standards for connecting to <Company Name>'s network from any host. These standards are designed to minimize the potential exposure to <Company Name> from damages which may result from unauthorized use of <Company Name> resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical <Company Name> internal systems, etc.

2.0 Scope
This policy applies to all <Company Name> employees, contractors, vendors and agents with a <Company Name>-owned or personally-owned computer or workstation used to connect to the <Company Name> network. This policy applies to remote access connections used to do work on behalf of <Company Name>, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

3.0 Policy
3.1 General
It is the responsibility of <Company Name> employees, contractors, vendors and agents with remote access privileges to <Company Name>'s corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to <Company Name>.
General access to the Internet for recreational use by immediate household members through the <Company Name> Network on personal computers is permitted for employees that have flat-rate services. The <Company Name> employee is responsible to ensure the family member does not violate any <Company Name> policies, does not perform illegal activities, and does not use the access for outside business interests. The <Company Name> employee bears responsibility for the consequences should the access be misused.
Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of <Company Name>'s network:
Acceptable Encryption Policy
Virtual Private Network (VPN) Policy
Wireless Communications Policy

Acceptable Use Policy

For additional information regarding <Company Name>'s remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

3.2 Requirements

Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.

At no time should any <Company Name> employee provide their login or email password to anyone, not even family members.

<Company Name> employees and contractors with remote access privileges must ensure that their <Company Name>-owned or personal computer or workstation, which is remotely connected to <Company Name>'s corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

<Company Name> employees and contractors with remote access privileges to <Company Name>'s corporate network must not use non-<Company Name> email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct <Company Name> business, thereby ensuring that official business is never confused with personal business.

Routers for dedicated ISDN lines configured for access to the <Company Name> network must meet minimum authentication requirements of CHAP.

Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

Frame Relay must meet minimum authentication requirements of DLCI standards.

Non-standard hardware configurations must be approved by Remote Access Services, and InfoSec must approve security configurations for access to hardware.

All hosts that are connected to <Company Name> internal networks via remote access technologies must use the most up-to-date anti-virus software (place url to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.

Personal equipment that is used to connect to <Company Name>'s networks must meet the requirements of <Company Name>-owned equipment for remote access.

Organizations or individuals who wish to implement non-standard Remote Access solutions to the <Company Name> production network must obtain prior approval from Remote Access Services and InfoSec.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

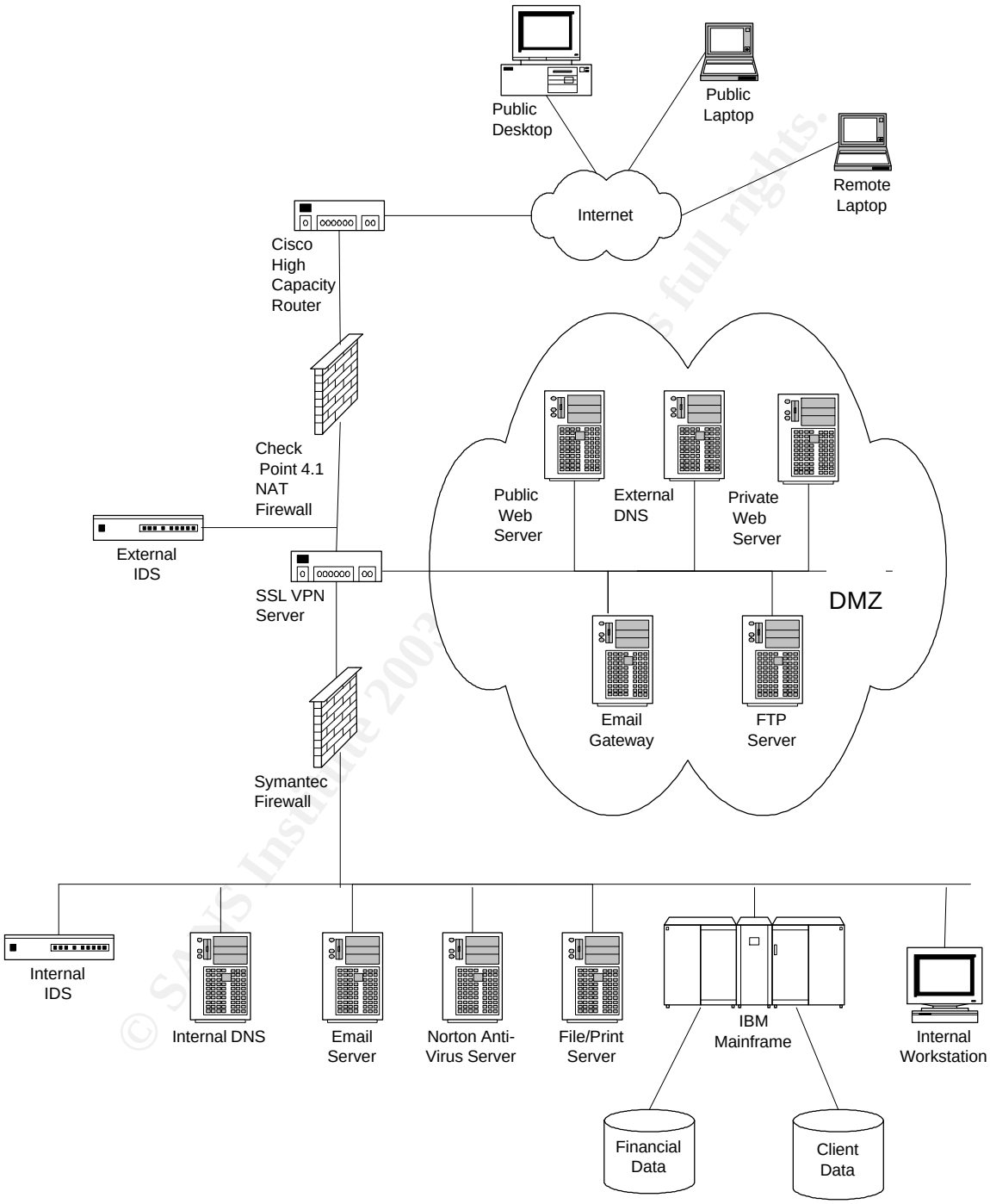
5.0 Definitions

Term	Definition
Cable Modem	Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.
CHAP	Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCIData Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.
Dial-in Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a <Company Name>-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into <Company Name> and an ISP, depending on packet destination.
DSL	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
Frame Relay	A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.
ISDN	There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.
Remote Access	Any access to <Company Name>'s corporate network through a non-<Company Name> controlled network, device, or medium.

Split-tunneling	Simultaneous direct access to a non-<Company Name> network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into <Company Name>'s corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

6.0 Revision History

Appendix C
The GIAC Group Infrastructure Diagram
Revised



Appendix D
The GIAC Group Infrastructure Description
Revisions

This appendix briefly describes the revisions to the IT infrastructure of The GIAC Group. Appendix C contains the revised infrastructure diagram.

- The Remote Access Server, the Cisco AS5300 has been removed. The new policy on remote access will no longer allow dial-up access to the corporate network. Access will be allowed only until the compliance date of the policy.
- Remote employees will use company-configured laptops. No personally owned workstations or laptops can be used after the policy compliance date.
- All remote employees will access the corporate network by means of a high-speed ISP through an Aventail EX-1500 SSL VPN appliance.
- A Symantec Enterprise Firewall 7.0 provides additional security between the DMZ and the internal network. Another layer of defense in depth is achieved. Have two different firewall vendors and rule sets to compromise from the perimeter.
- Added an external DNS and private web server to the DMZ. The security procedures implemented lays groundwork for the future for The GIAC Group by enabling secure web-access to data for clients and employees.

List of References

1) The SANS Institute, The SANS Security Policy Project URL: http://www.sans.org/resources/policies/Remote_Access_Policy.doc (06/20/2003)

2) Tech Target site for Security Professionals, searchSecurity.com Definitions, Peer-to-Peer definition URL: http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212769,00.html (08-12-2001)

3) Microsoft Corporation, HotFix & Security Bulletin Service, Microsoft Security Bulletin MS02-064 URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-064.asp (02/28/2003)

4) Tech Target site for Security Professionals, Quiz #27: Security Awareness for End Users URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci826572,00.html (05-31-2002)

5) Aventail site, Technical White Paper, "Comparing Secure Remote Access Options: IPSec VPNS vs. SSL VPNS", page 4, URL: http://www.aventail.com/downloads/pdfs/IPSECvsSSL_WP.pdf

6) Microsoft Corporation, Windows 2000 Professional Baseline Security Checklist URL: http://www.microsoft.com/technet/security/tools/chklist/w2kprocl.asp?frame=true (2001)

7) Microsoft Corporation, Microsoft Baseline Security Analyzer, internal help and homepage URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/mbsahome.asp (2003)

8) PestPatrol, Inc., Guidelines for initial testing of PestPatrol, page 1,3) URL: http://www.pestpatrol.com/ProductDocs/QuickStartGuide.pdf (2003)