Global Information Assurance Certification Paper

GIAC Enterprises

Security Policies and Procedures
For a Broadband Internet Service Provider

Bruce A. Kaalund
GISO –Basic Practical Assignment
Version 1.2 (February 9, 2002)

Table of Contents

ASSIGNMENT #1 – DESCRIBE GIAC ENTERPRISES 4

IT INFRASTRUCTURE 5
Market Segment *5*
Subscriber Facility 6
Local Aggregation Center 6
Market Aggregation Center 7
Support Data Center *8*
Purpose 9
BUSINESS OPERATIONS 11
Business Origins *11*
Culture *12*
Groups *12*
Management 12
Systems 13
Implementation 14
Operations 14
Network Security 15
Market *16*

ASSIGNMENT 2 – IDENTIFY RISKS 17

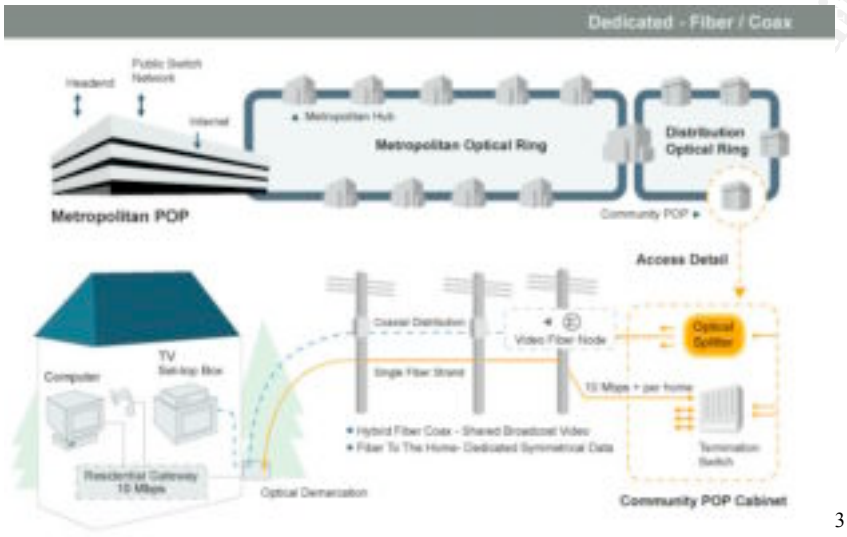
THE "CROWN JEWELS" 17
AREAS OF RISK 18
Unauthorized changes to network devices *18*
Overview 18
GIAC Enterprises Concern 18
Damage Potential 19
Occurrence Potential 20
Mitigation 20
Authorized remote access to network devices *21*
Overview 21
GIAC Enterprises Concern 21
Damage Potential 22
Occurrence Potential 22
Mitigation 22
Privileged Information *23*
Overview 23
GIAC Enterprises Concern 23
Damage Potential 24
Occurrence Potential 24
Mitigation 25

ASSIGNMENT 3 – EVALUATE AND DEVELOP SECURITY POLICY 26

EVALUATE SECURITY POLICY 26
Purpose *26*
Background *26*
Scope *27*
Policy Statement *27*
Responsibility *27*
Action *27*
Other *27*
REVISED SECURITY POLICY 28
ASSIGNMENT 4 – DEVELOP SECURITY PROCEDURES 30
APPENDIX A - REMOTE ACCESS POLICY 34
REFERENCES 44
INFORMATION FROM THE WORLD WIDE WEB 44
BOOKS 45

Assignment #1 – Describe GIAC Enterprises

GIAC Enterprises is a broadband cable television and Internet service provider. In contrast to the current model of broadband providers who use their existing (or upgraded) cable plant to provide both downstream cable television content and two-way Internet access, GIAC Enterprises is building their network using bundled coax/fiber-to-the-home technology. In this, it is similar to the type of service being provided by a Denver, CO based provider[1]. GIAC Enterprises provides " . . . a full spectrum of video, voice, and high speed data services, giving you the convenience of one-stop shopping and the value of a bundled service offering."[2] Below is a high-level diagram of the network.



[3]

Using standard coaxial cable, GIAC Enterprises can provide its subscribers many programming services, such as:

- Local Television Channels (ABC, NBC, CBS, Fox, WB, UPN, Public)
- "Superstation" Programming (WGN Chicago, WWOR New York)
- 50-premium movie channels (multiple instances of HBO, Shotime, Cinemax, Starz! The Movie Channel, etc)
- Pay-per-view and video-on-demand for feature length movies
- Subscription sports programming (NBA, MLB, NHL, NFL, ESPN, Fox SportsNet)

Using fiber-to-the-home technology, GIAC Enterprises can provide Internet access at 100 Mbps, with a 3-year upgrade path to 1 Gbps. Through the use of an Online Service Provider (OSP), GIAC Enterprises also provides e-mail, personal web space, file storage, and newsgroup access. The use of the fiber technology also allows GIAC Enterprises to

[1] Website: http://www.winfirst.com
[2] From http://www.winfirst.com/abt_winfirst/main.html
[3] Revised diagram from http://www.winfirst.com/abt_winfirst/technology.html

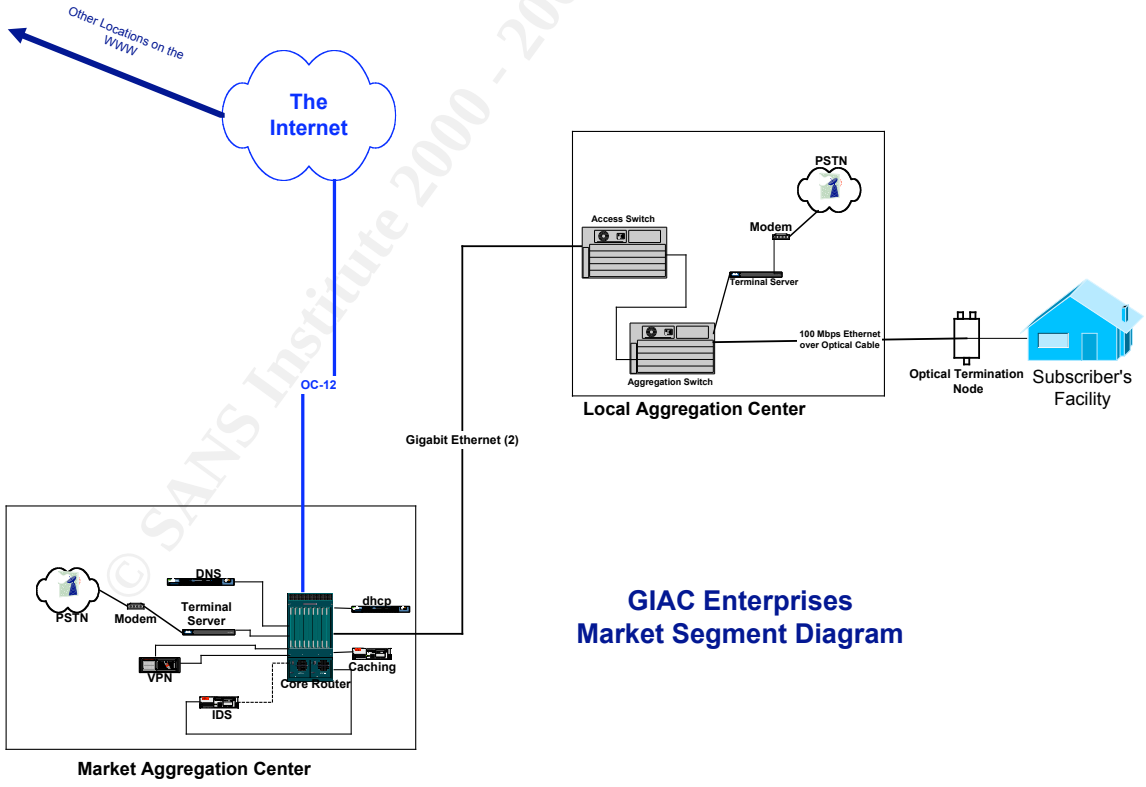
provide telephone services to the home, thereby serving as an alternative to the local telephone company.

IT Infrastructure

Because of the expensive nature of the services it provides, GIAC Enterprises decided to reduce capital cost by outsourcing its internal back office operations to an Applications Service Provider (ASP). The ASP is responsible for all aspects of the back office support, including security. This leaves GIAC Enterprises with the cable and Internet infrastructure. Professionals experienced in the operations of the infrastructure supporting the one-way video transmission maintain the cable portion, while a specialized group (described in the Business Operations section) maintains the IP Services portion of the network.

The IP Services portion of the network uses an address range for private networks in accordance with RFC-1918, and has ARIN-issued addresses for the subscriber computers, along with those devices facing the Internet. The infrastructure is broken into two segments, and is illustrated in the following diagrams:

Market Segment



The market segment of the network are divided into the following areas:

- Subscriber Facility
- Local Aggregation Center
- Market Aggregation Center

Within each location, GIAC Enterprises has supplied equipment that is under its responsibility. These devices are described in the following sections.

Subscriber Facility

The subscriber facility is normally the home. The subscriber facility has conduit used for the wires supporting existing telephone and/ or cable service. Assuming the existing CATV plant cannot be reused, GIAC Enterprises will pull the coax and optical fiber into the home through this conduit. The coax is terminated into the existing home CATV system. The optical fiber is terminated into the Cisco ONT 1031, which is an optical network terminator which " . . . provides a demarcation device for metro Ethernet access networks with Ethernet in the First Mile technology that can be managed completely remotely."[4] This is the demarcation point between the subscriber's home network or PC, and the GIAC Enterprises network. The Ethernet interface will receive a private address from the ESSC server, while the subscriber computers will receive a minimum of one public IP address, and more based on their subscription level. GIAC Enterprises responsibility for securing the network ends at the Ethernet interface to the ONT 1031; from that point on into the house, the subscriber is responsible for securing their equipment.

Local Aggregation Center

The optical fiber and coax cables are run back to the local aggregation center, which serves as a head end for the video (coax) portion of the service, and an aggregation (optical fiber) point for the data portion of the service. The optical fibers from the subscribers terminate into a series of Cisco Catalyst 4006 with high-density optical interface cards, serving as aggregation switches. A fully stocked switch will have 240 optical ports. Multiple 4006 switches will feed into a single 4006 serving as an access switch. This 4006 is configured with a gigabit card for connections from aggregation switches, and a single GBIC card that provides two-1 gigabit connections to the market aggregation center.

A terminal server, which is a Cisco 2620 with either a 16 port or a 32 port asynchronous card installed, provided emergency out-of-band access to the devices via the console port. The terminal server was connected to a modem, and a POTS line to the public telephone network. All devices in the local aggregation center have private IP addresses on their interfaces.

---

[4] Cisco ONT 1000 Gigabit Ethernet Series Data Sheet, Cisco Systems, Inc, page 1, found at http://www.cisco.com/warp/public/cc/so/neso/efmsol/ont1k_ds.htm

Market Aggregation Center

The market aggregation center is where all local aggregation centers feed into. It is here where the subscriber receives initial services, and gains access to The Internet. The gigabit feeds from the local aggregation centers connect into a Cisco 7204 VXR core router. This router will also have a blade for 100base-T connections to support the services provided at the market aggregation center, and a blade that provides access to the OC-12 IXC circuit to the Internet, these connections will have public IP addresses.

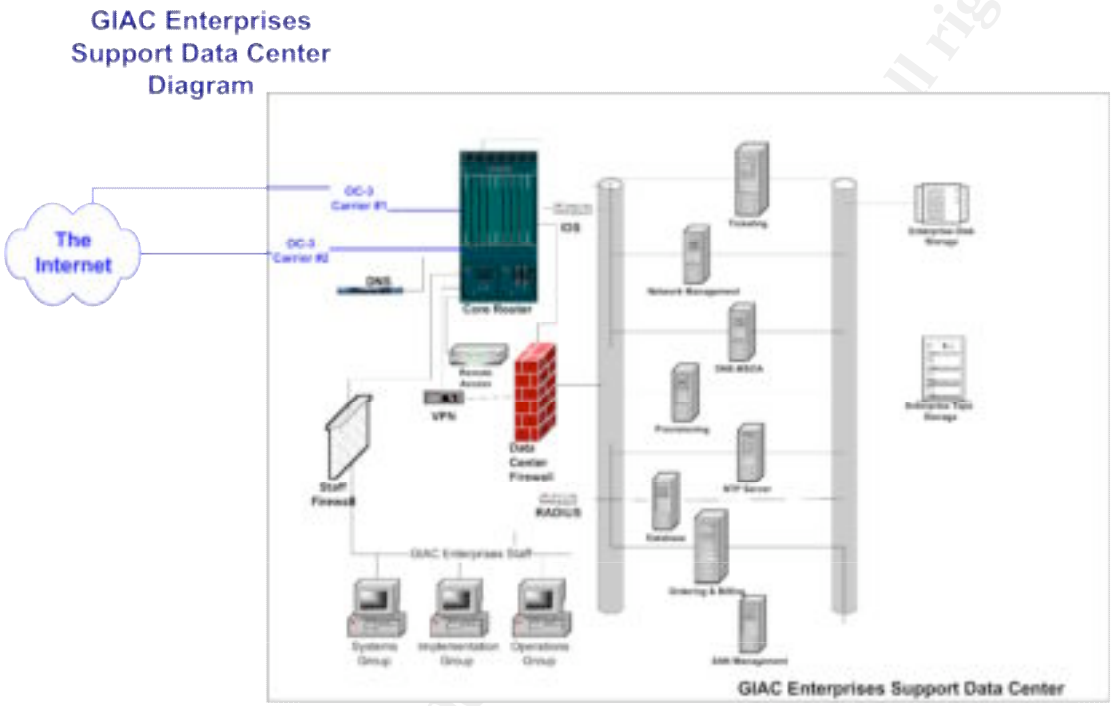
Connected to the 100base-T blade are the following services:

Service	Equipment & Application	Purpose	IP Addresses
VPN Appliance	Dual Linux servers running FreeS/WAN.	Transport management and support traffic between market aggregation centers and the support data center	Public and Private
Caching Servers	Multiple Linux servers running Squid	High-performance caching solution to optimize bandwidth savings.	Public
DHCP	Dual Linux servers running dhcpd with modifications	Provide public IP addresses to subscriber computers, after verification of MAC address of the ONT 1000 Ethernet port.	Private
DNS	Dual Linux servers running BIND 9	Local name server for subscribers in that market.	Public
Intrusion Detection	Single Linux server running Snort	Looking for potential attacks in progress on market devices with public addresses.	Private and Promiscuous
Terminal Server	Cisco 2620 with 32-port asynchronous card	Network and remote (via PSTN) console access to market devices	Private

Of particular interest is the VPN appliance. GIAC Enterprises decided to implement an internal backbone for management traffic (e.g., SNMP traps and queries) and support traffic (SSH access into a device) between the local and management aggregation centers and the support data center. Since the majority of devices in the aggregation centers have private IP addresses, and all of the devices in the support data center have private IP addresses, it became cost effective to use The Internet as a virtual backbone through the use of VPN technology. Using a self-hardened version of Linux running FreeS/WAN on Intel-based servers, GIAC Enterprises was able to construct an optimized VPN appliance platform that delivered throughput of 2Mbps from each market aggregation center.

Support Data Center

The support data center is used to house all of the support systems and personnel for the IP Services network.



The support data center is where all management information traffic from the local and market aggregation centers feed into. The dual OC-3 feeds from the Internet connect into a Cisco 7204 VXR core router. This router will also have two blades for 100base-T connections to support the services provided for the local and market aggregation centers, and for access to the support staff described in the Business Operations section.

The following devices are installed in the support data center:

Service	Equipment & Application	Purpose	IP Addresses
VPN Server	Dual Linux servers running FreeS/WAN.	Transport management and support traffic between market aggregation centers and the support data center.	Public and Private
Remote Access Appliance	Dual Nokia Crypto Cluster 2500	Remote access for authorized systems group personnel to work on troubles after hours	Public and Private
Data Center Firewall	Dual Linux servers running netfilter and iptables.	High-performance firewall allowing access to the data center backbone from the aggregation centers (via the VPN) and the GIAC Enterprises staff (uses NAT for Ntwk Mgmt and NTP servers).	Private
Staff Firewall	Dual Linux servers running netfilter and iptables.	High-performance firewall allowing access to the data center backbone, the aggregation centers (via the VPN) and The Internet (via NAT).	Private and Public
DNS	Dual Linux servers running BIND 9	Local name server for the support data center	Public
Intrusion Detection	Single Linux server running Snort	Looking for potential attacks in progress on all support data center devices. Uses port spanning on the core router.	Private and Promiscuous
Ticketing	Dual Sun Enterprise 420R running Solaris 8 and Remedy AR 5.0	Trouble ticket generation and knowledge base management	Private
Network Management	Single Linux server running OpenNMS	Provides near- real-time status and performance of all network devices (with public and private interfaces) using SNMP v3.	Private
DNS-SoA	Dual Linux servers running BIND 9	Serves as the source of authority for the GIAC Enterprises network.	Private

Service	Equipment & Application	Purpose	IP Addresses
RADIUS	Dual Linux servers running Livingston RADIUS	This is the primary source of AAA for all device access in the IP Services network.	Private
Provisioning	Multiple Cisco Ethernet Subscriber Solution Engines	Rack-mounted " . . . hardware-based network management tool that monitors Cisco ONT 1031s"[5] One device per two markets, based on Cisco spec of "Single-point management for up to 2000 Cisco ONT 1031 devices"[6]	Private
NTP Server	Single Linux server running ntpd.	Provides stratum 2 clock for the GIAC Enterprises IP Services network	Private
Database	Dual Sun Fire 880s running Solaris 8 and Oracle 8i	Provides database instances for ticketing, network management, and ordering and billing applications	Private
Ordering and Billing	Dual Linux servers running Apache and tools for XML design.	Internally developed XML front end to Oracle database for service ordering, subscriber management, and billing.	Private
Enterprise Disk Storage	Compaq StorageWorks Modular Array 8000	Used for disk storage via fiber-based storage area network	Private
Enterprise Tape Storage	ADIC Scalar 100	Used for tape backup via fiber-based storage area network	Private
SAN Management	Compaq SANworks Management Appliance Sun Netra t 1440 running Solaris 8 and ADIC Stornext Management Suite	Used for the management of the devices on the storage area network	Private

[5] http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/ftth/esse_isg/appl_ove.htm

[6] http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/ftth/esse_isg/appl_ove.htm

The Linux servers for applications in the market aggregation centers and the support data center are Compaq ProLiant DL 360, 380, and 580s.

The users comprising the Systems and Implementation groups in the GIAC Enterprises staff are equipped with Compaq Evo N160 laptops with 1GHz processors, 20 GB hard drives, and 512 MB of memory. These machines are running VMWare Workstation 3.0 supporting concurrent sessions of Windows 2000 Professional and SuSE 7.3 Linux Professional. The Operations group staff is equipped with Compaq D500 series desktop machines with 2.20 GHz processors, 20 GB hard drives, and 512 MB of memory. These machines are running Windows 2000 Professional.

Business Operations

In order to better understand the operations of GIAC Enterprises, we need to understand the origins of the company, and its culture.

Business Origins

GIAC Enterprises was founded in 1997 by a group of students at a major polytechnic university in Alabama. As juniors, they all were in a spring session class that looked at the business aspects of technology. The "group of twelve" as they are now known, were a diverse group of men and women with majors in Business, Accounting, Computer Science, Electrical Engineering, and Marketing. The major project for the class was to develop a business plan for a high-tech startup. Their business plan consisted of providing broadband entertainment and Internet access to homes in the affluent areas of Hoover AL (suburb of Birmingham) and the Buckhead area of Atlanta GA. They proposed doing this through the use of optical fiber technology, based on the concept of delivering "fiber-to-the-home". The "group of twelve" believed they would receive an "A" for their effort; however, their final grade for the project was a "B-". The stated reason for the lower grade was the team of professors did not believe that this plan could ever be implemented in real life. The group of twelve decided to prove the professors wrong.

Throughout the summer and their senior years, they worked on the business plan, refining it as they became aware of the latest technology. By the spring of 1997, they felt that they had a strong story to tell with their plan, and decided to test the venture capital market, which seemed to be looking to put dollars into Internet-based projects. To their surprise, they received funding from several organizations. A couple members of the group were also role players on the football and basketball teams, and they were able to convince some of their pro-bound teammates to invest in the project. The initial funding came to $1.2B. With that money, they set up shop in some office space in downtown Birmingham, hired some experienced professionals, and preceded to submit a winning bid to provide their services to three subdivisions in Hoover. In short, GIAC Enterprises became successful enough to secure additional funding, and spread out to additional

upscale suburban areas. GIAC Enterprises turned its first profit in 2001, and moved into their new facility in the Van Ness area of Washington DC.

Culture

Being a company created and run by young (under 30 years of age) professionals, these entrepreneurs are willing to think "outside of the box" on many issues, which helped with their conservative spending practices. Realizing that they would have to spend heavily on personnel (especially technical people) and that the cost of pulling fiber and coax would not be cheap, they decided to focus on the core of the business, (cable and ISP) and farm out everything else. For the business back office and other ancillary services (i. e., e-mail services) the business side of the group won the argument, and secured favorable contracts for outsourcing. This allowed GIAC Enterprises to minimize the number of technical and administrative personnel they needed to hire, along with the costs of benefits that support personnel, such as insurance.

Following in this mode, the technical leadership decided to be selective in where they spent the bulk of their funds. In order to have a strong infrastructure, they built their network on what they felt was best of breed equipment from Cisco, and used strong vendors for key parts of the infrastructure (ADIC, Oracle, Compaq). However, for the hosts that would support the ISP, they built upon open source products, using Linux as the operating system of choice. All systems were built using applications such as BIND, OpenNMS, and dhcpd. The hiring of extremely sharp and very experienced developers and engineers allowed them to develop the systems under an aggressive schedule with a minimum of problems. The initial development meant many nights of pizza and beer, but they were able to develop, document, and implement systems that held up very well in production. In short, they felt that they could do almost anything!

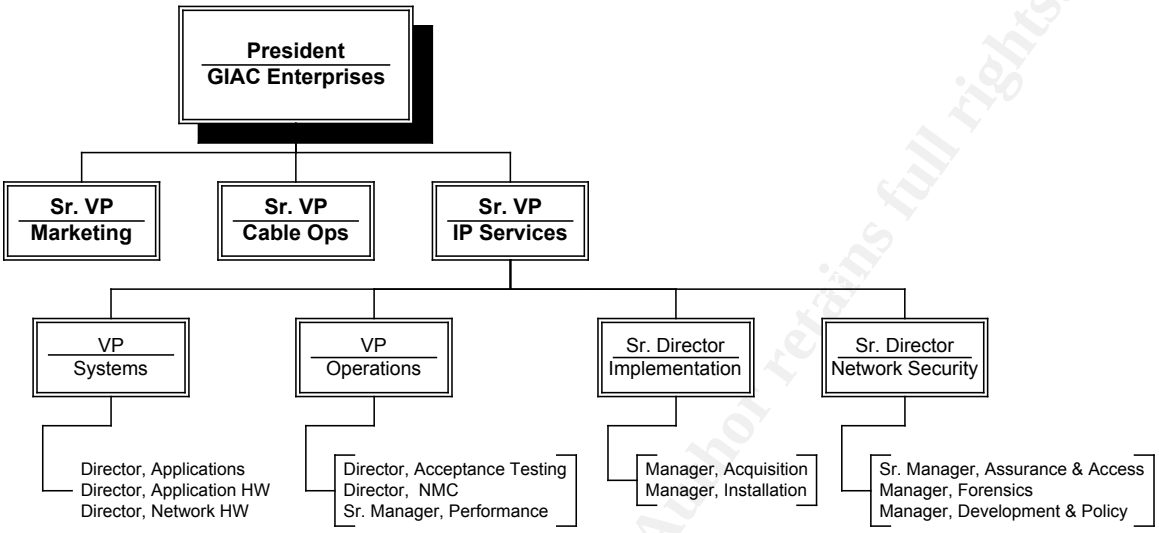
Groups

Being an ISP, GIAC Enterprises is focused on providing broadband access to the Internet to its subscribers. Its major functions cover operations, systems, and implementation of the systems that directly support the network. It was stated earlier that GIAC Enterprises had outsourced the operations and housing of the traditional internal back office systems and functions to an ASP. In addition, they have outsourced some "traditional" ISP services (e-mail, personal web space, etc.) to an OSP. Besides being very cost effective, the outsourcing of the non-core functions allows GIAC Enterprises to focus directly on the network.

Management

The management structure of GIAC Enterprises is pretty straightforward. The President of the company has three direct reports; Senior Vice President of Cable Operations, Senior Vice President of IP Services, and Senior Vice President of Marketing. The whole organization chart is shown in the diagram below.

This paper is concerned with the IP Services division. The groups that report to the Sr. Vice President of IP Services are described below.



Systems

The systems group is responsible for the sizing and specification of the network that feeds into the market aggregation centers. This encompasses the sizing of the switches in the centers, along with the server and VPN devices. They are also responsible for the specification and sizing of the IXC circuits connecting the market aggregation centers to The Internet. These engineers and system administrators are the highest level of maintenance support when the equipment goes down. When the operations group can't correct a problem, it is escalated to the systems group for their expert knowledge.

The systems group is also responsible for the systems in the data center that support the whole network. The system administrators and applications experts support the DHCP scopes, assure the proper entries are in the DNS servers throughout the network, and perform operating system installs on all host equipment.

The majority of the work is done at the Van Ness facility. Engineers are expected to have privileged access to the equipment they have expertise for, whether in production, or in the off-line lab. Because they serve as the escalation group for operations, they are on a rotating on-call schedule. All access to the devices is through using secure shell, which all devices provide at some level. Because of the cost of living in Washington, DC, all of the engineers and system administrations live far (35+ miles) away. Therefore, remote access to the systems on the network is important.

The Vice-President of Systems heads the systems group. Her direct reports are the Director of Applications, the Director of Application Hardware (servers, operating

systems), and the Director of Network Hardware (switches, routers, terminal servers, VPN appliances).

Implementation

After systems perform the sizing and specification of devices and/or circuits, that information is passed to the implementation group. This group has relationships with multiple equipment vendors, and all IXC's, and is able to place orders for gear and circuits via secure web-based ordering systems. The implementation group also runs the warehouse, where equipment is delivered, the hardware configured, a minimum software configuration installed, and the equipment powered up and allowed to burn in for 72 hours. After burn-in is complete, the implementation group securely crates the equipment, and has it shipped to its final destination. When the equipment reaches its destination, implementation works with the local site technicians to have the equipment "racked and stacked", cabled, and powered up. After passing installation tests, the implementation group installs the final software configuration, using configurations on their laptop they received from the systems group. Last, the implementation group performs initial acceptance testing on the equipment. Once this has been successfully completed, they call the operations group to complete acceptance testing, and to place the equipment into production status.

The Senior Director of Implementation runs this group. His direct reports are the Manager of Acquisition (system ordering, warehouse management) and the Manager of Installation (burn-in, shipping, and site installation).

Operations

The operations group is responsible for the day-to-day operations of the network. The acceptance team receives the handoff of installed equipment from the implementation group. They will perform the final tests to accept new equipment into the network and prepare it for production status by installing the production passwords and SNMP community strings. At this point, the acceptance team will place the system into production.

Once it is in production status, it is handed off to the network management center (NMC), which is a 24-hour operation. The NMC monitors the systems for traps and faults using SNMP-based tools. Should equipment fail, or perform at a less than optimal level, it is their responsibility to open a trouble ticket, troubleshoot and resolve the situation. In many cases, the problem can be rectified by the network management center. If they are unable to rectify the problem, they can escalate the trouble ticket to the systems group for their expertise. The NMC will retain ownership of the trouble ticket, and remain in contact with the systems group until the problem is resolved. Only then, will the NMC close the trouble ticket, after documenting the solution.

Operations also have a performance team. Their responsibility is to collect the data from the network management system, and compile it into metrics reports that clearly illustrate

how well or poorly the network is performing. These reports are sent to senior management for their evaluation.

The Vice-President of Operations runs this group. His direct reports are the Director of Acceptance Testing, the Director of the NMC, and the Senior Manager of Performance.

Network Security

Network security is responsible for the management of risk mitigation for the IP Services network. In this function, the Senior Director of Network Security serves as the Security officer for the ISP, and as the security advisor to the Sr. VP of IP Services. In this function, Network Security develops security policies, administers equipment that supports the policies, and performs investigative work when the policies have been breached.

The assurance and access group is the largest shop in network Security. This function is responsible for the following tasks:

- Management of the support data center firewalls;
- Management of the IP Services VPN;
- Metric collection to assure the ongoing security of the network devices, through tasks such as regular port scanning and comparison of hashes of password files;
- Ownership and management of passwords and their creation;
- Control of providing access to devices, through management of RADIUS and remote access.

The forensics group is the shop that "plays with the hackers". They are the ones who watch for potential attacks, respond when an attack is in progress, and perform the collection of evidence after an attack is over or stopped. This team is responsible for the following tasks:

- Management of the intrusion detection system;
- Performance of random, unannounced penetration testing of markets;
- Interfacing with local, state and federal law enforcement authorities and responding to official court documents;
- Leadership of the Computer Emergency Response Team, which is made up of members of multiple organizations, which respond to incidents in progress and after the fact.

The last group is the development and policy group. This shop develops policies, standards, and audit procedures for the IP Services. They also are responsible for the security education program, which involves regular "lunchtime security briefs" where the IP Services members are presented security items they need in their daily work. This shop also attends new product team meetings to understand the products being developed, in order to assure that security is built in before going into production.

The Senior Director of Network Security heads this shop. His direct reports are the Senior Manager of Assurance and Access, the Manager of Forensics, and the Manager of Deployment and Policy.

Market

GIAC Enterprises is headquartered in Washington, DC, and serves the high-end suburban market place. Because of the cost of installing fiber optic cable to the home, and providing the electronics to make the solution work, it was decided to sell first to those homes that could afford such a premium service. GIAC Enterprises is presently providing service to the following markets:

Potomac, MD	Great Falls VA	Leawood (Kansas City) KS
Buckhead, (Atlanta) GA	Greenwich CT	Hockessin (Wilmington) DE
Hoover (Birmingham) AL	West Chester PA	Moorestown NJ
Belle Meade (Nashville) TN	East Hampton, NY	Beavercreek (Dayton) OH

The subscriber households in these communities have a minimum gross income of $250K, with a composition of two professional parents with an average number of children of 2 boys and one girl. GIAC Enterprises averages 1000 subscribers from each market. Based on the success of the product, GIAC Enterprises is forecasting moving into twelve more high-end markets over the next three years, in such areas as Boston MA, Charlotte NC, Chicago IL, Miami FL, and Dallas-Ft. Worth TX. GIAC Enterprises is also looking at providing fiber-based services to private student (off-campus) housing supporting major universities in the Ivy League, Big Ten, ACC, SEC, and Big East conferences.

Assignment 2 – Identify Risks

There are multiple areas of risk to an ISP. It is important to define the priorities for securing an ISP. According to Geoff Huston, these are the priorities for an ISP:

Integrity of the service. *The ISP has to protect the integrity of the network service and must be able to make the operation of the network relatively secure. This extends not only to the routers and switching elements of the network but also to the protection and integrity of the service delivery host platforms, including DNS servers, mail servers, Web servers, and caches, and any other service platforms operated by the ISP.*

Client security. *As well as protecting its own service assets from intrusion and disruption, the ISP is expected to assist clients (subscribers) to secure their operation from security incidents. This can take various forms, but normally does not extend all the way to have the ISP assume all responsibility for client network security. However, in certain areas, the client must trust the ISP's integrity of operation in order to implement its own security policy . . .*

Incident response. *When security incidents occur there is the expectation that the ISP will assist clients and peer ISPs in the tracing of such incidents to their source. Equally, where various forms of denial-of-service attacks are experienced, the ISP should assist in the removal of the attack, either through blocking the traffic or through identification of the source of the attack.*

Legal obligations. *Underpinning this is the ISP's legal and regulatory obligations, which may include the requirement to report criminal activity and cooperate with law-enforcement agencies in the investigation of such incidents.*[7]

The "Crown Jewels"

Based on the priorities listed above, GIAC Enterprises has determined that *Integrity of the service* is the most important priority. Remember, this service is offered to subscribers in a very high-income bracket, who are paying premium fees. Disruptions in service lead to refunds of the fees in accordance with the length of time the disruption was in effect. Multiple disruptions lead to the subscriber viewpoint of poor service, which leads to subscribers canceling for another provider. Both issues directly hit the bottom line.

Therefore, GIAC Enterprises has defined the markets (e.g., market aggregation centers and local aggregation centers) to be the crown jewels of the company. Loss of the support data center may mean that customer records can't be accessed, or new subscribers cannot be turned on, but the existing subscribers can still "surf the web", and

[7] Huston, Geoff, ISP Survival Guide, Strategies for Running a Competitive ISP, 1999, John Wiley & Sons, Inc., pp.351-2

access their e-mail from the OSP. However, the loss of a local aggregation center may mean loss of service for a few hundred subscribers; loss of a market aggregation center may mean the loss of service for more than a thousand subscribers. Both events can mean loss of revenue, as these subscribers are demanding, and can afford the legal support to back up those demands. Loss of service can also precipitate negative publicity in the media, as a major outage gets news coverage, and can generate political pressure from State Attorney Generals looking to get refunds, or elected legislators calling for investigations and hearings. All of the above can have an adverse effect on the bottom line, and can drive an ISP out of business.

Areas of Risk

Based on the knowledge that threats to the markets can create the most difficulty for GIAC Enterprises, the Network Security group has listed these issues as the most pressing to the organization:

- Unauthorized changes to network devices
- Authorized remote access to network devices
- Privileged Information

A discussion of each issue follows.

Unauthorized changes to network devices

Overview

Network devices in production status will eventually need attention. Whether it is a fault or performance issue, a necessary change mandated by a software bug or a new capability, someone must gain access to the device and make the configuration. Of course, that someone must be a person who is authorized to 1) access the device to make change and 2) be authorized to make the specific change. The staff of GIAC Enterprises residing in the support data center has that authorization. But, before a change is made, the change must pass muster in the change control process. Unauthorized changes are those that do not follow the change control process.

GIAC Enterprises Concern

Changes to devices from the support data center bring concerns. You cannot allow everyone in the support data center to have access to all devices. Too many people having the ability to make changes to a device can create problems with device performance that become difficult to troubleshoot. Therefore, only personnel designated with the responsibility for the service provided by the device will have the authority to access that device.

In addition, GIAC Enterprises must not allow access to the devices from other Internet users. This would place the devices at risk for being accessed and/or manipulated by

anyone from subscribers to "script kiddies" to hard-core hackers. This would create an environment where anyone could shut down the network by getting onto a device and making changes to its configuration.

Last, only approved changes can be done to the device. This change must receive technical review to assure proper testing and to validate the need to change a device in production. Random changes are not allowed, as they may not be technically sound, and may create problems that did not exist before the change, and may be very difficult to correct.

Although the above concerns appear to be more operational, they become security issues when a change is made to a device without authorization, and the ability to track that change back to an individual is not there. Such a change now appears as a breach, because it can't be verified to be an authorized change. This then becomes a security concern, as the network security group must investigate to see if this was a hack, and to determine if any damage had been done. Following proper change control procedures, this would be recognized as an error, and handled as such by the people who made the change.

Damage Potential

High. Many of GIAC Enterprises technical staff comes from the "dot-com" world. Many of these enterprises (no longer in existence) had young, energetic staff, fueled by coffee, cola and Chinese food to get their web sites up and running. Discipline was rarely instituted, and techies made changes when they wanted, without much testing or verification. A change made to a device that caused the device to fail became an issue for other techs when it occurred; lack of documentation and/or procedure led to the inability to distinguish the problem as a hack or a change gone awry.

Also, the issue of the disgruntled employee comes into play. According to the 2001 CSI/FBI Computer Crime and Security Survey, disgruntled employees ranks either first or second (in comparison to independent hackers) in the likely sources of attack over a five-year period.[8] GIAC Enterprises has a number of employees working long hours to get the job done. This produces a fair amount of fatigue and stress, which leads to frustration and poor performance. There have been staff firings due to poor performance, and the concern centers around the knowledge of the network and devices these people had at the time of their release. Good change control practices (along with other best practices for HR and security) allow GIAC Enterprises to quickly identify malicious changes to network devices by unhappy employees.

[8] Computer Security Institute, 2001 CSI/FBI Computer Crime and Security Survey, *chart, Likely Sources of Attack*, Page 9. Found at http://www.gocsi.com/press/20020407.html

Occurrence Potential

High. The occurrence potential is more an operational issue than a security issue. An engineer sees a problem, thinks they know the answer, and goes in and makes the change. They do not go through the change control procedure, because it takes too long (in their perception) to document the change, and to get the necessary approvals. This tends to occur when a bug is identified in software, and a patch is released with the bug announcement. The engineer takes the patch, installs it, and thinks all is fine. Multiple patches and or changes to the configuration to "tweak" the performance can go unnoticed until something goes wrong. Then an engineer looks at the configuration, notices changes that are not documented, and calls in security, because it appears to be a hack. In addition, the lack of such controls makes it easy for a disgruntled employee to go in and set a "time bomb" on key systems that would disrupt the performance of the network. Such mischief is a security issue, though it has its origins in operational procedures.

Mitigation

The mitigation of this problem has many parts:

1. *Strict adherence to the change control process.* This is the first line of defense to unauthorized changes. A change to a device's configuration must be documented, and reviewed by a board that can evaluate the change based on its necessity, and its potential for success. A change to one device may have a negative effect on another device in the network, which may create a performance issue in the network. Any change that is made to a device that does not have an approved change request is unauthorized, and will subject the perpetrator to punishment.
2. *Strong access controls.* Only authorized personnel should access equipment. A DNS engineer has no need to access the core router. This is based on the principle of least access; a person should only have the minimum access necessary to perform their tasks, and should only be granted to those devices for which that person holds responsibility. AAA (Authentication, Authorization, Accounting) systems such as RADIUS. RADIUS offers tight security, flexibility, simplified management and extensive logging capabilities.[9] This allows GIAC Enterprises to provide user ID and password authentication, and to limit authorization to equipment by user ID. It also allows GIAC Enterprises to develop an audit trail listing who accessed the device and at what time.
3. *Documented HR Processes.* It is very important to have strong HR processes for new employees and for departing employees. New employees should have documentation completed by their supervisor specifying what access they should be authorized for. Upon separation of the employee from GIAC Enterprises, all authorized access must be revoked on the day of separation. This will alert security to be more vigilant about this employee, by monitoring their access

[9] RADIUS Administrator's Guide, 950-1206A October 1996, Overview; http://docs.daphnis.com/portmaster/RADIUS/guide/1overview.html

closely. This may help to mitigate widespread damage from a disgruntled employee. For employees being terminated for cause, an expedited process must be in place. Upon removal from the premises, all access must be revoked, and a review of the devices the terminated employee had access to would be reviewed for changes.

Authorized remote access to network devices

Overview

The same network devices in production status will eventually need attention during non-working hours. Because much of the staff live a great distance from the office (due to the cost of living in Washington DC) it is not always feasible to make them come in to fix a problem. The time lost in driving (up to one hour one way) is not effective, especially if the problem takes five minutes to fix. Therefore, the systems and operations groups successfully petitioned for the use of remote access for their people. Now, issues can be dealt with from the staff person's home. Of course, that staff person must be a person who is authorized to access the device to make changes. That authorization is based on the principle of least access, described by Randall Nichols, et al.[10] This remote access is only to be used for accessing devices on the IP Services network. Other business functions (e-mail, file transfer, web surfing, etc.) are strictly prohibited.

GIAC Enterprises Concern

Remote access is very problematic. The biggest issue is GIAC Enterprises loses control of the device accessing the network. Unless the company provides the staff person a laptop for working away from the office and specifies that all access to the network away from the office is to be done using that laptop, the network will be accessed using a personal machine. Use of the personal machine brings the issue of abuse by someone other than the support person. It becomes easy for a child to use the machine, and get access to the network simply because the intended user either did not disconnect from the remote access, or they left the password in clear view. In addition, should the support person (or another user with access to the machine) be suspected of hacking the network, the PC would have to be subpoenaed, as GIAC Enterprises cannot walk into a person's home and take their personal equipment. Therefore, a laptop issued by the company is a safe alternative, but is subject to theft, and the issues it brings.[11]

Another concern is the handling of company business across the Internet. It is very probable that the support staff do not live in the upscale areas where GIAC Enterprises provides its service. So, they have to get their own Internet access whether it is dial-up, ISDN, xDSL, or cable modem. GIAC Enterprises has no way of verifying the security of

[10] Nichols, Randall K, et al, Defending Your Digital Assets Against Hackers, Crackers, Spies & Thieves, 2000, The McGraw-Hill Companies, Inc., pg 102
[11] Fowler, Dennis, Virtual Private Networks, Making the Right Connection, 1999, Morgan Kaufmann Publishers, Inc. pg 176

the network their employees are using from home. Therefore, it is possible that someone has places a sniffer in the ISP network a support person is using, and is capturing valuable passwords, user IDs, and configurations for the GIAC Enterprises network. Control of anti-virus is another concern. Corporate-sponsored laptops can have their virus signatures updated every time the machine is connected to the corporate network. Home PCs do not have that guarantee. Poor virus protection can lead to the spread of viruses from the home.

Damage Potential

High. Anyone accessing the network remotely could do so without the controls that are in place at the support data center (i.e., firewalls, AAA, etc.). This would allow a person to access the devices on the network (provided they either had the user Ids and passwords) or to give them the time to run brute force cracking software against the devices.[12] A successful cracking session would provide access to the devices, where changes could be made in violation of change control procedures (if done "legitimately" by a support person) or through a hack.

Occurrence Potential

High. Let's look back at the first issue, and recognize that the staff is still having the "dot-com" mentality. They will fix the problem first and ask permission later, if they bother. Doing it from home means they can do these things without oversight. Children left alone will explore, and if they can get into a place where they shouldn't (which remote access provides) they will and possibly create havoc. Again, any sort of hack or unauthorized change can lead to degradation or disruption of service, affecting the bottom line.

Mitigation

The major mitigation procedure is to assure that only authorized people can access the network via remote access, and that they are limited to their area of responsibility. This means the network security group would have to practice compartmentalization. This practice, as described by Paul Strassmann, " . . . requires deliberate and pre-planned isolation of access to only those data that can be associated with designated persons and their 'need to know.'"[13] Therefore, a formal application and approval process must be developed for service personnel to gain access to the network remotely. This would cover GIAC Enterprises employees, along with contractors and/or consultants who are performing staff augmentation functions.

---

[12] Hatch, Brian, et al, Hacking Linux Exposed, Linux Security Secrets and Solutions, 2001, The McGraw-Hill Companies, page 289

[13] Paul A. Strassmann, Executive Security Briefing: How to manage remote workforce security, 23 Oct 2001. http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci777355,00.html

To mitigate the transmission of company business across the Internet, a VPN solution should be developed. Because the developers did not want to tackle the development of a Windows client for FreeS/WAN, GIAC Enterprises is using the Nokia Crypto Cluster 2500 for remote VPN access. The Crypto Cluster will provide the following:

1. The creation of IPSEC packets on the laptop. This way, the packets enter the Internet in IPSEC format;
2. Use of Triple DES as the encryption algorithm;
3. Generation and use of X.509 digital certificates for the IKE key exchange;
4. Support for RADIUS authentication;
5. Limit use of the VPN to specific host groups,
6. Will not impede regular web surfing over the user's ISP access.

Last, the policy for remote access will have to clearly state, that the VPN client will only be installed on a GIAC Enterprises-provided laptop, or a consulting/contracting firm laptop. The client shall not be installed on a personal computer belonging to the staff person, or any one else. This will help to mitigate the potential for other persons using the VPN to access the network (whether by accident or intentionally), and will simplify the forensics process in the event a support member is suspected of using the VPN for sinister purposes. It also helps with the HR issue, in that the laptop is recovered upon termination, thereby securing the VPN access.

Privileged Information

Overview

Passwords are a way of life with network equipment. Cisco switches and routers have passwords for console access, which allow read-only access to a limited set of information, and the enable level, which allows one to do any and everything to the device as far as the configuration. Linux and UNIX hosts have various levels of access, depending on how the privileges were set up. They also have the root access, which, like Cisco's enable, allows one to do any and everything to the device's configuration. SNMP is very important to GIAC Enterprises, as the network management system uses SNMP to receive traps created by system faults or warnings, and other components of the device MIBs to measure device performance.

GIAC Enterprises Concern

Because GIAC Enterprises uses RADIUS for read-only authentication, the concern is limited to what are referred to as "Privileged Information". This consists of the root password, the Cisco enable password, and the SNMP community strings.

Any one with knowledge of either the enable or the root password can access the respective device, and make changes to the configuration. This includes those changes which are of a devious nature, such as removing access control list statements on a router that deny access to the device directly from the Internet, or changing the root password

to something no one else knows. Should a user gain root access they could place a Trojan program or a root kit on the device, and use it as a source for launching attacks on the GIAC Enterprises network, or on other networks. In addition, any member of the support staff could use their knowledge of the root or enable passwords to make configuration changes without getting change control approval.

Another concern on passwords is the tendency to make them easy to remember. Nichols, et al, say, "When system users are allowed to select their own passwords, they naturally opt for easily remembered constructions. This leads to two related problems: easily guessed passwords and the use of dictionary words."[14] Unfortunately, this also makes them easy to guess using software crackers. Hatch, et al discusses what comprises a bad password.[15]

Community strings, have a default configuration from the factory of "public" for read-only access, and "private" for read-write access.[16] There are multiple tools that will exploit this, and they exist (at no cost) on the web.

Damage Potential

Very High. Passwords are the last line of defense when it comes to network equipment. If a hacker has broken through all other lines of defense, strong, difficult to guess passwords are all that protects the device from either being made to crash, or being used as a tool to attack other devices and/or networks. SNMP community strings, particularly the read-write string, can provide someone the ability to make key configuration changes across the network without detection. Either result can result in degradation or disruption of service to the subscribers, affecting both the bottom line, and the service reputation.

Occurrence Potential

Very High. Weak passwords are listed as one of SANS 20 most critical Internet security vulnerabilities.[17] Use of default SNMP community strings also appears on the SANS top 20.[18] The occurrence potential is such, because " . . . the majority of successful attacks on computer systems via the Internet can be traced to exploitation of security flaws . . ."

---

[14] Nichols, Randall K, et al, Defending Your Digital Assets Against Hackers, Crackers, Spies & Thieves, 2000, The McGraw-Hill Companies, Inc., pg 256

[15] Hatch, Brian, et al, Hacking Linux Exposed, Linux Security Secrets and Solutions, 2001, The McGraw-Hill Companies, page 306

[16] McClure, Stuart, et al, Hacking Exposed, Network Security Secrets and Solutions, 3rd Edition, 2001, The McGraw-Hill Companies, pp. 449-50

[17] *Vulnerability G2 – Accounts with No Passwords or Weak Passwords*, from The SANS Institute, The Twenty Most Critical Internet Security Vulnerabilities (Updated), The Experts Consensus, Version 2.100, October 2, 2001, Found at http://www.sans.org/top20.htm

[18] *Vulnerability U7 – Default SNMP Strings*, from The SANS Institute, The Twenty Most Critical Internet Security Vulnerabilities (Updated), The Experts Consensus, Version 2.100, October 2, 2001, Found at http://www.sans.org/top20.htm

on the SANS list.[19] These are among the attacks used by "script kiddies" utilizing the plethora of freeware tools found on the web. Gaining access is the fourth step in the anatomy of a hack,[20] and that can be accomplished either through passwords or community strings.

Mitigation

GIAC Enterprises has developed a strong process for privileged information. First, all privileged information (passwords and community strings) are "owned" by network security. Network security creates them, installs them on new equipment, and updates them across the network via scripts. All passwords are administered by the NMC. When support personnel need to make a change to a device, they must contact the NMC for the password. The NMC verifies the person, checks to see if they are supposed to access the device at that time (access granted either through an approved change request or through an open trouble ticket), and then reveals the necessary password. The NMC then submits a request to network security to change the password on that particular device, which happens within 24 hours. The risk of a support person using that password before the password is changes is mitigated by the fact that they have to authenticate to the RADIUS server before accessing the device, and Tripwire is being run on all hosts.

Network Security generates all passwords and community strings using a software package called *quicky password generator*.[21] The specifications on the passwords are; eight characters, upper and lower case, alphanumeric. This prevents common words or easy passwords from being created. All privileged information is changed every 90 days.

In addition, all access to network devices is through secure shell (SSH). Telnet, because it transmits in the clear, has been prohibited on the network. SSH encrypts the path to the device, providing additional protection.

[19] Opening Page, The SANS Institute, The Twenty Most Critical Internet Security Vulnerabilities (Updated), The Experts Consensus, Version 2.100, October 2, 2001, Found at http://www.sans.org/top20.htm

[20] McClure, Stuart, et al, Hacking Exposed, Network Security Secrets and Solutions, 3rd Edition, 2001, The McGraw-Hill Companies, inside back cover.

[21] Found at: http://www.quickysoftware.com

Assignment 3 – Evaluate and Develop Security Policy

For this section, the sample policy we are using is based upon policy in use at the author's company. The sample policy also contain information taken from the sample policies found on the SANS web site.[22]

Evaluate Security Policy

For GIAC Enterprises, we will develop a remote access policy from an existing policy. The policy to be evaluated for development can be found in Appendix A. It has been edited to remove any corporate-identifying information.

Overall, it is a good document. The issue with this document is it combines policy, standards, and procedure into one document, without clear delineation. According to Christopher King, et al, "Policies are higher level documents that do not specify technologies, but focus on addressing a complete picture . . . A policy not only explains the how, but also the why, provides a stronger baseline for people to follow, and through this simple education it enables people to understand the goal of the security program."[23] This policy is very close to the position GIAC Enterprises takes for its remote access. However, due to its "jack-of-all-trades" nature, it is not a document that can stand alone as a policy. This document will need to have some re-working in order to be used for GIAC Enterprises. The format to be used will be based on the format for the Sample Remote Access Policy created by SANS.[24]

We will now evaluate the document for the presence of some key issues.

Purpose

This policy does have a purpose (paragraph 2.1). It is to the point, indicating that its purpose is " . . . to define requirements for connecting to (the) network from a remote location".[25] However, it is not specific enough, as this statement could refer to an individual or to another company. For GIAC Enterprises, the focus will have to be much more narrow, that is, focus on the support personnel. A policy for remote access for companies doing business with GIAC Enterprises will be a separate document.

Background

This policy does not have a background. Although it is not necessary, it would help with clarity if one were included. The policy for GIAC Enterprises will include a background.

---

[22] Found at http://www.sans.org/newlook/resources/policies/policies.htm
[23] Christopher M King, et al, Security Architecture, Design, Deployment & Operations, 2001, The McGraw Hill Companies, pg 13
[24] Found at http://www.sans.org/newlook/resources/policies/policies.htm
[25] Appendix A, paragraph 2.1

Scope

This policy does have a scope (paragraph 2.2). It is a very good scope, in that it explains the extent of the policy, and delineates who and what is covered. In addition, the last paragraph allows for the introduction of other technologies into the remote access umbrella. This is good, should GIAC Enterprises find it worthwhile to allow other types of access. GIAC Enterprises will use this scope in its entirety.

Policy Statement

The policy statement is mixed in the section called Responsibilities (section 3). Therefore, the policy statement is not clearly delineated. It appears that the most useful language for the policy statement starts in paragraph 3.2, General Responsibilities. Looking at the wording, these appear to be in line with the overall policy of GIAC Enterprises. However, we will have to clearly label it as the policy statement, and assure that the wording portrays a clear statement.

Responsibility

Section 3 has a lot of responsibility statements in it. Much of this section (save for those paragraphs being used for the policy statement) can be used by GIAC Enterprises with the necessary modifications. However, paragraph 3.3.1 needs to be placed in the procedure document, while much of section 3.3 will be moved under responsibilities.

Action

There is no action section in this document. However, actions and responsible parties have their definitions scattered throughout sections 4 (Qualification Criteria), 5 (Activation and Termination), and 6 (Remote Access VPN Process). GIAC Enterprises will have to ferret this information out, and place it under the requirements section.

Other

There needs to be a section delineating who is qualified to receive access to the remote access, and for what duration. This will fall into the requirements section, and will borrow from section 4. The version and status information are important, and should be included in a header. The table of contents should not be included. The document information (section 1.1) is also not necessary, although the owner can be included in the header. The rest of this document is more geared to procedure. They will not be included in the GIAC Enterprises policy document.

Revised Security Policy

GIAC Enterprises
Remote Access Policy
Version: 1.0, Final Edition, April 26, 2002
Owner: Senior Director, Network Security

Purpose
The purpose of this policy is to define requirements for GIAC Enterprises support personnel needing to connect to the IP Services network from a remote location. These policies are designed to minimize the potential exposure to GIAC Enterprises from damages that may result from unauthorized use of GIAC Enterprises resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical GIAC Enterprises internal systems, etc.

Background
The devices in production status on the GIAC Enterprises IP Services network need attention during non-working hours. Due to the distance key staff may live from the support data center, and the need to solve outages quickly, it is not always feasible to have them come in to work on a problem after business hours. Therefore, GIAC Enterprises has provided the capability of remote access for their people

Scope
This policy applies to all GIAC Enterprises employees, contractors, vendors and agents with a GIAC Enterprises-owned or contractor-owned laptop computer used to connect to the IP Services network. This policy applies to remote access connections used to do work on behalf of GIAC Enterprises.

Remote access implementations that are covered by this policy are virtual private network (VPN) technology, dial-in modems, frame relay, ISDN, DSL, and cable modems, etc. NOTE: GIAC Enterprises only allows remote access through the GIAC Enterprises-provided VPN.

Policy
General

- It is the responsibility of GIAC Enterprises employees, contractors, and consultants (collectively known as users) with remote access privileges to the IP Services network to ensure that their remote access connection is given the same consideration as the user's on-site connection to GIAC Enterprises.
- General access to the Internet for recreational use is not permitted. The user is responsible to ensure that any person other than the support person to whom the computer was assigned does not use this access in violation of any GIAC Enterprises policies, does not perform illegal activities, and does not use the access for outside business interests. The user bears responsibility for the consequences should the access be misused.
- For details of protecting information when accessing the IP Services network via remote access, please refer to the GIAC Enterprises Intranet site (w3.giacenterprises.com/security/policy/)
- Network Security has the responsibility for the operation and maintenance of the remote access. Network Security will implement, provision, and maintain the devices and software used for the remote access VPN.

Requirements

- Remote access must be strictly controlled. Control will be enforced via the use of a software client provided by network security; access will be controlled by RADIUS.
- At no time should any user provide his or her login or password to anyone, not even family members.
- All remote access to the IP Services network must be done from a GIAC Enterprises provided laptop or, in the case of consultants or contractors, a consulting firm provided or contracting firm provided laptop. The use of computers purchased for personal use (desktop or laptop) is strictly forbidden.
- Users with remote access privileges must ensure that their company-owned laptop computer, which is remotely connected to the IP Services network via the Internet, is not connected to any other network (i.e., home network) at the same time.
- The remote access is only to be used to access devices on the IP Services network. No other functions (e-mail, file server access, etc.) shall be performed over this access.
- Non-standard hardware configurations must be reviewed, tested, and its configuration documented and approved by network security before it is allowed to access the IP Services network remotely.
- All hosts that are connected to the IP Services network via remote access must use the most up-to-date anti-virus software, and must be scanned for viruses on a weekly basis.
- GIAC Enterprises staff members are authorized to use the remote access VPN, provided they have a GIAC Enterprises-issued laptop, and can access the Internet from home via a recognized ISP. GIAC Enterprises support staff will re-qualify every year.
- Co-op students working for GIAC Enterprises as staff members are authorized to use the remote access VPN provided they have a GIAC Enterprises-issued laptop, and can access the Internet from home via a recognized ISP. Co-op students will re-qualify every six (6) months.
- Consultants and contractors (hereafter referred to as Consultants) serving as temporary support personnel with GIAC Enterprises can be authorized access to the remote access VPN network if they meet the following criteria:
    - Work for a GIAC Enterprises approved firm;
    - Have permission from a Senior GIAC Enterprises manager, (Director or above);
    - Can access the Internet via a ISP.

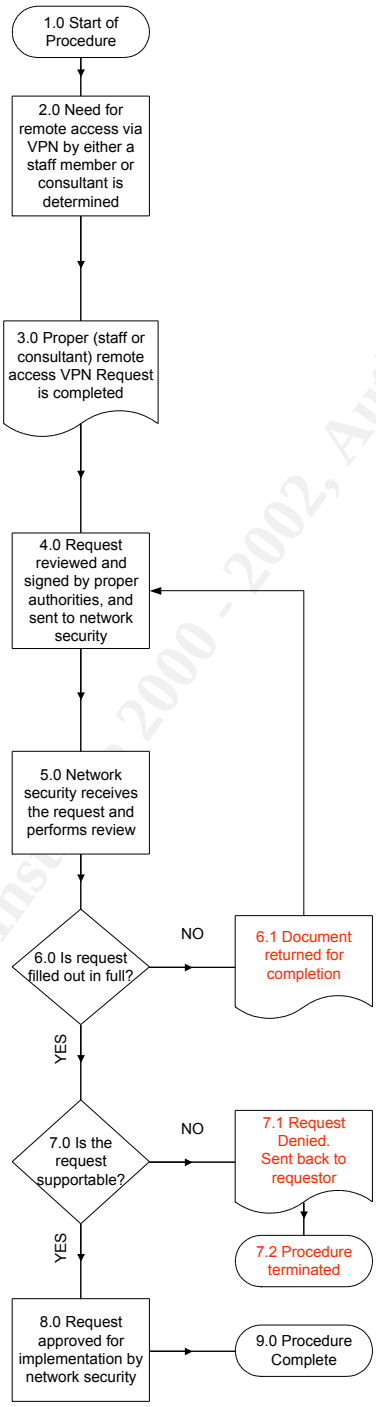
Enforcement
Any employee found to have violated this policy might be subject to disciplinary action, up to and including termination of employment.

Revision History

Date	Person Responsible	Revision
26 Apr 02	Director, Network Security	Initial final document

Assignment 4 – Develop Security Procedures

The procedure that will be developed is the procedure for obtaining remote access. The procedure is illustrated in the following flowchart.



The procedure is now discussed in detail.

Step 1.0 – *Start of Procedure.* This is the entry point for the remote access VPN approval.

Step 2.0 – *Need for remote access via VPN by either a staff member or consultant is determined.* The staff member's reporting manager, or the GIAC Enterprises reporting person the consultant is assigned to must determine this need. The need is based upon the fact that the person needing the access is both authorized to work on the equipment the particular group is responsible for, and is a participating member of the group's on-call rotation.

Step 3.0 – *Proper (staff or consultant) remote access VPN Request is completed.* The person desiring the access must fully complete the proper request form. There is a different request form for internal support staff, and for consultants or contractors. The following information must be included in the completed form:

FOR STAFF PEOPLE:
- Full name of the staff member;
- Office address, phone number, and GIAC Enterprises e-mail address;
- Department, name of Manager and/or Director;
- GIAC Enterprises file number (this is used for identification when calling into the NMC to get a privileged password [root or Cisco enable] to perform the task);
- Home address and phone number;
- Type of access at home (e. g., CATV company cable modem, Verizon DSL, etc.);
- Type (e. g., Dell Latitude) and serial number of the BLANK-issued laptop;
- NIC card type (e. g., Xircom RealPortTM CardBus Ethernet 10/100+Modem56), and the MAC address of that NIC that is installed in the laptop;
- Detailed description of the business need for access to the RAVPN.

FOR CONSULTANTS AND CONTRACTORS:
- Full name of the Consultant;
- GIAC Enterprises office address, phone number, and GIAC Enterprises e-mail address;
- GIAC Enterprises department, name of GIAC Enterprises Manager and/or Director;
- Home address and phone number;
- Type of access at home (e. g., CATV company cable modem, Verizon DSL, etc.);
- Name of Consulting or Contract firm the person represents, along with address phone number, and firm e-mail address;
- Consulting firm partner or contracting firm's representative name, address phone number, and e-mail address;
- Type (e. g., Dell Latitude) and serial number of the firm-issued laptop;
- NIC card type (e. g., Xircom RealPortTM CardBus Ethernet 10/100+Modem56), and the MAC address of that NIC that is installed in the laptop;

- Detailed description of the business need for access to the RAVPN.

For consultants and contractors, network security will create a special number to be used for identification when calling into the NMC to get a privileged password [root or Cisco enable] to perform the task. This number will be completed after the request is approved.

In addition, the remote access acknowledgement form must be signed. This form is attached to the Remote Access VPN Usage Policy document, and states that the requestor understands the policy and agrees to comply with the policy.

Step 4.0 – *Request reviewed and signed by proper authorities, and sent to network security.* Once the request has been completed, and the remote access acknowledgement form signed, the requestor must take the form to the proper authority. This is either the manager or director of the department the requestor is assigned to. In order to expedite the request, it is the responsibility of the manager or director, to assure the following:

- The document is completed in full;
- The requestor has signed the document;
- For consultants/contractors, that the representative of the contracting or consulting firm has signed the form;
- The detailed description of the business need has been completed and is clear;
- The remote access acknowledgement form has been signed.

Once the above have been completed, the document is sent to the network security department.

Step 5.0 – *Network security receives the request and performs review.* Once network security receives the request, it performs a review of the document. Network security looks for the following:

- All forms have been turned in;
- The document is completed in full (no blank spaces);
- The requestor has signed the forms;
- The people who have the authority to sign have signed the document;
- The business need is valid and supportable;

The reviewing official is the Senior Director, Network Security.

Step 6.0 – *Is the request filled out in full?* Network security must assure that the forms are completed in full. Every spot on the form must be answered, as the information is vital to knowing who the person is, where the person will be using the remote access, and what equipment the user is using. The MAC address will be used in forensics should the user be suspected of improper use of the remote access. The remote access acknowledgement must also be completed. Incomplete forms will be returned to the

manager or director of the requestor for completion, as indicated by *sub-step 6.1 – Document returned for completion*.

Step 7.0 – *Is the request supportable?* Network security must then determine if the request can be supported. Issues that would make the request unsupportable are:

- Use of a Non-GIAC Enterprises laptop;
- Use of a non-consulting firm issued or non-contracting firm issued laptop;
- Business reason that does not cover the support needs of the IP Services network (e.g., e-mail access, newsgroup access);
- Refusal to provide information required on the request form;
- Refusal to sign the remote access acknowledgement form.

The request will be denied, and the forms sent back to the requestor, as indicated by *sub-step 7.1 – Request Denied*. Sent back to requestor. The procedure would then be terminated, as indicated by *sub-step 7.2 – Procedure Terminated*.

Step 8.0 – *Request approved for implementation by network security.* If the request meets the necessary requirements, the Senior Director, Network Security will approve it, and deliver it to the assurance and access group for implementation.

Step 9.0 – *Procedure Complete.* This procedure is complete. The next process is the Remote Access Implementation Procedure.

Appendix A - Remote Access Policy

Remote Access Policy

Version: 1.0

Status: Final

Date: April 8, 2002

TABLE OF CONTENTS

1 DOCUMENT CONTROL 4
1.1 DOCUMENT INFORMATION 4
1.2 SUMMARY DOCUMENT REVISION HISTORY 4
1.3 DOCUMENT STATUS 4
1.4 REFERENCES 4
1.5 GLOSSARY 5
2 INTRODUCTION 7
2.1 PURPOSE 7
2.2 SCOPE 7
3 RESPONSIBILITIES 8
3.1 OVERALL RESPONSIBILITY 8
3.2 GENERAL RESPONSIBILITIES 8
3.3 REQUIREMENTS 8
3.3.1 Remote Access Client Software 9
4 QUALIFICATION CRITERIA 10
4.1 BLANK STAFF 10
4.1.1 Hardware and Software Requirements 10
4.1.2 Period of Use 10
4.1.3 Information Needed by Network Security 10
4.1.4 BLANK Co-Op Students 11
4.1.5 BLANK File Number 11
4.2 CONTRACTORS AND CONSULTANTS 11
4.2.1 Hardware and Software Requirements 11
4.2.2 Period of Use 11
4.2.3 Information Needed by Network Security 11
5 ACTIVATION AND TERMINATION 13
5.1 ACTIVATION 13
5.2 TERMINATION 13
5.2.1 For BLANK Staff Members 13
5.2.2 For Consultants and Contractors 13
6 REMOTE ACCESS VPN PROCESS 14
6.1 RAVPN CREATION & ISSUANCE 14
7 APPENDIX A - REQUEST FOR BLANK STAFF MEMBER ACCESS TO RAVPN 16
8 APPENDIX B - REQUEST FOR CONSULTANT/CONTRACTOR ACCESS TO RAVPN 17
9 APPENDIX C - REMOTE ACCESS POLICY ACKNOWLEDGEMENT FORM 19

1 Document Control

1.1 Document Information
Title: Remote Access Policy Document
Author: Bruce Kaalund
Owner: Bruce Kaalund
For approval by: Bruce Kaalund

2 Introduction
2.1 Purpose
The purpose of this policy is to define requirements for connecting to BLANK's network from a remote location. These policies are designed to minimize the potential exposure to BLANK from damages which may result from unauthorized use of BLANK resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical BLANK internal systems, etc.

2.2 Scope
This policy applies to all BLANK employees, contractors, vendors and agents with a BLANK-owned or contractor-owned laptop computer used to connect to the BLANK network. This policy applies to remote access connections used to do work on behalf of BLANK, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy are specific to remote access via virtual private network technology via dial-in modems, frame relay, ISDN, DSL, and cable modems, etc. NOTE: BLANK only allows VPN Remote Access.

3 Responsibilities
3.1 Overall Responsibility
BLANK has the responsibility for the operation and maintenance of the BLANK High Speed Data network. This involves the need to access various pieces of equipment on the network even when not at the BLANK facility in LOCATION. In order to provide access to those who are authorized to operate and maintain the equipment remotely, a remote access virtual private network (RAVPN) has been created.

The owner of the RAVPN is Network Security (NS). NS will implement, provision, and maintain the devices and software used for the RAVPN

3.2 General Responsibilities
It is the responsibility of BLANK employees, contractors, and consultants (collectively known as users) with remote access privileges to BLANK's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to BLANK.

General access to the Internet for recreational use by immediate household members through the BLANK Network on personal computers is not permitted. The user is responsible to ensure the family member does not violate any BLANK policies, does not perform illegal activities, and does not use the access for outside business interests. The user bears responsibility for the consequences should the access be misused.

3.3 Requirements
The following are requirements for use of the RAVPN:

* Remote access must be strictly controlled. Control will be enforced via the use of a software client provided by NS; access will be controlled by digital certificates and/or RADIUS.
* Only devices allowed to have the RAVPN software client installed will be company-provided (BLANK, consultant, or contractor) laptops. Home or personal laptops, desktops or workstations are not authorized remote access to the BLANK network.
* The RAVPN is set up to be used for maintenance and can only access IP Addresses in the BLANK network's private IP address range.
* At no time should any user provide their login or email password to anyone, not even family members.
* Users with remote access privileges must ensure that their company-owned laptop computer, which is remotely connected to BLANK's corporate network, is not connected to any other network at the same time.
* Users with remote access privileges to BLANK's corporate network must not use non-BLANK email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct BLANK business, thereby ensuring that official business is never confused with personal business.
* Non-standard hardware configurations must be reviewed, tested, and its configuration documented and approved by NS before it is allowed to access the network remotely.
* All hosts that are connected to BLANK internal networks via remote access technologies must use the most up-to-date anti-virus software, and must be scanned for viruses on a weekly basis.

3.3.1 Remote Access Client Software
The VENDOR client is the software that will be used for remote access to the BLANK network. NS will provide this software at the time of installation, along with a digital certificate that specifies the policies that allow the user access to the network. A NS engineer will do configuration and installation of all RAVPN software. Neither the client nor the digital certificate is to be removed or transferred to another machine without the written approval of NS management and direct involvement of a NS engineer.

4 Qualification Criteria
There are certain criteria that must be met in order to receive access to the RAVPN network. These criteria are listed below.

4.1 BLANK Staff
BLANK staff can qualify for access to the RAVPN network if they meet the following criteria:

* Full-time employee of BLANK (does not include co-op students, see 4.1.4);
* Have permission and a demonstrated need to access devices and/or services under the responsibility of BLANK from a remote location;
* Can access the Internet via the BLANK network, or from a recognized Internet Service Provider (ISP);

4.1.1 Hardware and Software Requirements

The staff member must have a BLANK-issued laptop computer in order to have the client software installed. Home personal computers shall not have access to the RAVPN under any circumstances. The laptop shall meet the following minimum requirements:

* Microsoft Windows(r) 95/98/2000 or Windows NT with Service Pack 4 or later;
* 4MB of available hard disk space;
* 64 MB of RAM

4.1.2 Period of Use
The period of qualification BLANK staff shall be granted access to the RAVPN shall be one year. Each year, the staff member shall re-qualify for access to the RAVPN. Failure to re-qualify shall result in termination of the staff member's access to the RAVPN.

4.1.3 Information Needed by Network Security
In order for access to be granted to the RAVPN, the staff member must complete the BLANK Remote Access VPN Request Form with the following information:

* Full name of the staff member;
* Office address, phone number, and BLANK e-mail address;
* Department, name of Manager and/or Director;
* BLANK file number (used for telephone authentication, see 4.1.5)
* Home address and phone number;
* Type of access at home (e. g., BLANK cable modem, Verizon DSL, etc.);
* Type (e. g., Dell Latitude) and serial number of the BLANK-issued laptop;
* NIC card type (e. g., Xircom RealPortTM CardBus Ethernet 10/100+Modem56), and the MAC address of that NIC that is installed in the laptop (Do not use the MAC address of the NIC on the docking station).

This document, along with the signed original BLANK Remote Access Policy Acknowledgement Form, must be signed by the staff member, and their Manager and/or Director.

4.1.4 BLANK Co-Op Students
BLANK co-op students must meet the same criteria as BLANK staff members. The only difference is their access shall be limited to six months.

4.1.5 BLANK File Number
The BLANK file number will be used by the ESC for authentication when a staff member requests access to a device by calling the ESC on the telephone. The BLANK file number is a number created by BLANK, and is unique to every employee.

4.2 Contractors and Consultants
Consultants and contractors (hereafter referred to as Consultants) to BLANK can qualify for access to the RAVPN network if they meet the following criteria:

* Work for a BLANK approved firm;
* Have permission and a demonstrated need to access devices and/or services under the responsibility of BLANK from a remote location;
* Can access the Internet via the BLANK network, or from a recognized Internet Service Provider (ISP).

4.2.1 Hardware and Software Requirements
The Consultant must have a firm-issued laptop computer in order to have the client software installed. Home personal computers shall not have access to the RAVPN under any circumstances. The laptop shall meet the following minimum requirements:

* Microsoft Windows(r) 95/98/2000 or Windows NT with Service Pack 4 or later;
* 4MB of available hard disk space;
* 64 MB of RAM.

4.2.2 Period of Use
The maximum period of qualification BLANK Consultants shall be granted access to the RAVPN shall be three (3) months. Every three months, the Consultant shall re-qualify for access to the RAVPN. Failure to re-qualify shall result in termination of the Consultant's access to the RAVPN.

4.2.3 Information Needed by Network Security
In order for access to be granted to the RAVPN, the Consultant must complete the BLANK Remote Access VPN Request Form for Consultants with the following information:

* Full name of the Consultant;
* BLANK office address, phone number, and BLANK e-mail address;
* BLANK department, name of BLANK Manager and/or Director;
* Home address and phone number;
* Type of access at home (e. g., BLANK cable modem, Verizon DSL, etc.);
* Name of Consulting or Contract firm the person represents, along with address phone number, and firm e-mail address;
* Consulting firm partner or contracting firm's representative name, address phone number, and e-mail address;
* Type (e. g., Dell Latitude) and serial number of the firm-issued laptop;
* NIC card type (e. g., Xircom RealPortTM CardBus Ethernet 10/100+Modem56), and the MAC address of that NIC that is installed in the laptop (Do not use the MAC address of the NIC on the docking station);
* Detailed description of the business need for access to the RAVPN.

This document, along with a signed original BLANK Remote Access Policy Acknowledgement Form must be signed by the Consultant, the BLANK Manager and/or Director they report to, and the consulting firm partner or contracting firm representative.

5
Activation and Termination

No access to the RAVPN will be given unless the completed forms, along with the required signatures, are presented to Network Security. Prior to installation and activation, the request will be reviewed and approved by:

* For BLANK Staff -- Manager, Security Assurance;
* For Contractors and Consultants - Director, Network Security

5.1 Activation
Upon approval, the person requesting access to the RAVPN will be directed to present their laptop to a designated Security Engineer, who will install the client and digital certificate on that person's laptop. The requestor will also receive printed instructions on using the RAVPN. Any questions shall be directed to the Security Assurance team.

5.2 Termination
The access to the RAVPN shall be terminated under the following conditions:

5.2.1 For BLANK Staff Members
* Termination of the BLANK staff member;
* Transfer of the staff member from BLANK;
* Failure to re-qualify at the end of one year
* Violation of the responsibilities listed in section 3 of this document;
* Any performance or security violation done while using the RAVPN

5.2.2 For Consultants and Contractors
* Termination of the consultant or contractor from their firm;
* Termination of the consultant or contractor from the BLANK contract;
* Failure to re-qualify at the end of three (3) months;
* Violation of the responsibilities listed in section 3 of this document;
* Any performance or security violation done while using the RAVPN

6 Remote Access VPN Process
The issuance of RAVPN is described in the following process:

6.1 RAVPN Creation & Issuance
The following process will govern the creation and issuance of RAVPN:

CHART REMOVED

* Need for remote access via VPN by either a staff member or consultant is determined - Managers need to make a careful analysis of who needs to have remote access to the network. Criteria should include whether the person involved will be charged with on-call status, whether the person has the expertise to work independently on network devices, and the distance they live from the Cherry Hill facility.

* Proper (staff or consultant) RAVPN request is completed - For each person a manager desires to have remote access, a request must be completed in full, including all signatures. In addition, the user must return the signed BLANK Remote Access Policy Acknowledgement Form. The proper form must be completed for BLANK staff, co-op students, or consultants or contractors. The completed documents are then to be sent to the Director, Network Security, or Manager Security Assurance.

* Is the request filled out in full? - Network Security will review the request for completeness and clarity. Any request that is not fully completed will be returned to the requestor to be completed. Once complete, the request can be re-submitted to Network Security for consideration.
* Is the request supportable? - All fully completed requests will then be evaluated to see if Network Security can support the request. Non-supportable requests can include remote access into PPT, for example. If the request cannot be supported, it will be denied and sent back to the requestor. Network Security will discuss all denied requests with the requestor, to see if an alternative can be found.

* Request sent to Security Assurance for Implementation - If approved, the request will be forwarded to an engineer in Security Assurance.

* Security Assurance prepares certificate and VPN client - The Security Assurance engineer will prepare the digital certificate and VPN client in preparation for installation onto the user's certified laptop.

* Security Assurance installs certificate and client on laptop - Within 1-5 business days, Security Assurance will contact the user via e-mail to let them know that we are ready to install the client and certificate. The user will have to bring their laptop to Security Assurance so the engineer can install the client on the machine.

7
Appendix A - Request for BLANK Staff Member Access to RAVPN

8
Appendix B - Request for Consultant/Contractor Access to RAVPN

9
Appendix C - Remote Access Policy Acknowledgement Form

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

2.0 Scope
This policy applies to all BLANK employees, contractors, vendors and agents with a BLANK-owned or contractor-owned laptop computer or workstation used to connect to the BLANK network. This policy applies to remote access connections used to do work on behalf of BLANK, 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. NOTE: BLANK only allows VPN Remote Access.

3.0 Policy
3.1 General
1. It is the responsibility of BLANK employees, contractors, vendors and agents with remote access privileges to BLANK's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to BLANK.
2. General access to the Internet for recreational use by immediate household members through the BLANK Network on personal computers is not permitted. The BLANK employee is responsible to ensure the family member does not violate any BLANK policies, does not perform illegal activities, and does not use the access for outside business interests. The BLANK employee bears responsibility for the consequences should the access be misused.

3.2 Requirements
1. Secure remote access must be strictly controlled. Control will be enforced via Digital certificates and the use of RADIUS.
2. At no time should any BLANK employee provide their login or email password to anyone, not even family members.
3. BLANK employees and contractors with remote access privileges must ensure that their BLANK-owned or personal computer or workstation, which is remotely connected to BLANK's corporate network, is not connected to any other network at the same time.
4. BLANK employees and contractors with remote access privileges to BLANK's corporate network must not use non-BLANK email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct BLANK business, thereby ensuring that official business is never confused with personal business.
5. Routers for dedicated ISDN lines configured for access to the BLANK network must meet minimum authentication requirements of CHAP.
6. Frame Relay must meet minimum authentication requirements of DLCI standards.
7. Non-standard hardware configurations must be approved by Remote Access Services, and InfoSec must approve security configurations for access to hardware.
8. All hosts that are connected to BLANK internal networks via remote access technologies must use the most up-to-date anti-virus software .

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
BLANK provides 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. DLCI Data 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 BLANK-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into BLANK 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 BLANK's corporate network through a non-BLANK controlled network, device, or medium.

Split-tunneling
Simultaneous direct access to a non-BLANK network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into BLANK'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 Acknowledgement

I have read the BLANK Remote Access Usage Policy. I understand the contents, and I agree to comply with the said Policy.

Name:

Location:

Signature:

Date:

1 An approved firm is defined here as a firm which has an approved and signed Master Services Agreement with BLANK

References

Information from the World Wide Web

Western Integrated Networks. Available at
http://www.winfirst.com

Cisco ONT 1000. Available at
http://www.cisco.com/warp/public/cc/so/neso/efmsol/ont1k_ds.htm

Cisco Ethernet Subscriber Solution Engine. Available at
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/ftth/esse_isg/index.htm

Cisco 4000 Optical Network Terminal. Available at
http://www.cisco.com/warp/partner/synchronicd/cc/pd/si/casi/ca4000/sales/efm4k_ql.htm

Cisco 4000 Switch. Available at
http://www.cisco.com/univercd/cc/td/doc/pcat/ca4000.htm
http://www.cisco.com/warp/customer/cc/pd/si/casi/ca4000/prodlit/c4ksw_pl.htm

Cisco 7200 Router. Available at
http://www.cisco.com/univercd/cc/td/doc/pcat/7200.htm

ADIC Stornext Management Suite. Available at
http://www.adic.com/ibeCCtpItmDspRte.jsp?minisite=10000&respid=22372&item=22961&section=10112

Compaq SANworks network appliance. Available at
http://www.compaq.com/products/sanworks/managementappliance/description.html
http://www.compaq.com/products/quickspecs/10547_na/10547_na.html

Compaq StorageWorks Modular Array 8000. Available at
http://www.compaq.com/products/quickspecs/10545_na/10545_na.html
http://www.compaq.com/products/storageworks/ma8kema12k/description.html

System Administrator – Security Best Practices. Available at
http://rr.sans.org/practice/sysadmin.php

The SANS Security Policy Project. Available at
http://www.sans.org/newlook/resources/policies/policies.htm

The SANS Institute, The Twenty Most Critical Internet Security Vulnerabilities (Updated), The Experts Consensus, Version 2.100, October 2, 2001. Available at http://www.sans.org/top20.htm

Paul A. Strassmann, Executive Security Briefing: How to manage remote workforce security, 23 Oct 2001. Available at http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci777355,00.html

RADIUS Administrator's Guide, 950-1206A October 1996, Overview. Available at http://docs.daphnis.com/portmaster/RADIUS/guide/1overview.html

Computer Security Institute, 2001 CSI/FBI Computer Crime and Security Survey. Available at http://www.gocsi.com/press/20020407.html

Books

King, Christopher M, Curtis E. Dalton, and T. Ertem Osmanoglu, Security Architecture, Design, Deployment & Operations, 2001, The McGraw Hill Companies

McClure, Stuart, Joel Scambray, George Kurtz, Hacking Exposed, Network Security Secrets and Solutions, 3rd Edition, 2001, The McGraw-Hill Companies

Hatch, Brian, James Lee, George Kurtz, Hacking Linux Exposed, Linux Security Secrets and Solutions, 2001, The McGraw-Hill Companies

Nichols, Randall K, Daniel J, Ryan, and Julie J.C.H. Ryan, Defending Your Digital Assets Against Hackers, Crackers, Spies & Thieves, 2000, The McGraw-Hill Companies, Inc

Fowler, Dennis, Virtual Private Networks, Making the Right Connection, 1999, Morgan Kaufmann Publishers, Inc.

Huston, Geoff, ISP Survival Guide, Strategies for Running a Competitive ISP, 1999, John Wiley & Sons, Inc.