Global Information Assurance Certification Paper

Information Security Design for the CISO of a Professional Services Organization

Basic Practical Assignment
Version 1.1
For GIAC GISO Certification

January, 2002

Information Security Design for the CISO of a Professional Services Organization

Outline

I. GIAC Enterprises

Overview

Business Operations
1) **Culture**
2) **Go To Market Strategy**
3) **Organization**

IT Infrastructure
1) **Summary**
2) **Walkthrough**
   Internal Applications
   External Applications
   Operations
   Information Security
   Network Design

II. Security Policies

Risks
1) **Access and Authentication of Remote Users.**
2) **Asset management of clients connecting to the Corporate Network.**
3) **Malicious attacks on the IT Infrastructure.**
4) **Alliance partner network control.**
5) **Encryption and Proper Security of Data.**

Policies
1) **Remote Authentication and Access.**
2) **Desktop Management.**
3) **Encryption of Privileged and Confidential Data for Exchange Via Email.**

III. Security Procedures

1) **Desktop Management Procedures: Anti-virus software.**

Figures

I. GIAC Enterprises

The professional services industry has significantly changed in the past 20 years. Gone are the days of the "Big 8" when each company was a private partnership with a seemingly unlimited growth potential. During the halcyon days of the "Big 8", the bread and butter business unit, the audit practice, fed the growth of the newer sibling business units, tax and management advisory services. As the base of the U.S. economy evolved from a high labor content and manufacturing foundation to a technology and global foundation, the youngest sibling within the "Big 8" family, advisory services, shifted its focus to information technology consulting. IT consulting served as the profit engine that propelled the leading members of the "Big 8" to wealth and impacted the industry irrevocably.

To remain competitive, trailing members of the "Big 8" committed a once unthinkable action – they merged. The "Big 8" was gone, but the changes continued. The explosive adoption of the World Wide Web and the Internet computing module not only fed the consulting profit engine, but it created internal dissension and discord. Renegade consulting units bucked for more control and capital to fund their growth. The subsequent result was the breakup of numerous firms. But, the changes in culture and form did not stop there. The renegade consulting groups went further - to the open market for funding in the form of an Initial Public Offering. Not only were the "Big 8" consolidated and split by internal dissent, but the base form of the partnership, so revered in the halcyon days, was replaced with the cold structure of a publicly traded corporation.

GIAC Enterprises is one of the renegade consulting firms gone public. It split from its parent firm in 1998 under the terms of a less than amicable divorce. To fund its surging capital needs to compete during the Dot-Com craze of 2000, the leadership of company chose to go public. As a result, GIAC Enterprises was born.

Overview

GIAC Enterprises has over 40,000 employees (called associates) in the United States. In 2001, GIAC had revenue of $5.4 billion.

Once an independent entity, GIAC Enterprises expanded into alliances and joint ventures in the technology arena that were forbidden during their years as part of a "Big 8". As a result, the revenue derived by service offering illustrates that GIAC is a company with many different revenue streams:

- IT consulting (integration, custom development) 64%
- IT hosting/outsourcing 8%
- Software sales 15%
- Alliance royalties and earnings 13%

While consulting remains the major revenue stream, the other divisions' growth rates are higher. This is not by mistake, but is part of the overall GIAC strategy to grow beyond its traditional income stream.

Business Operations

Prior to discussing the IT Infrastructure, it is important to understand the business operations and culture of GIAC Enterprises.

Culture

The culture of GIAC Enterprises can be summarized by its motto: *"Respect and Serve: People – Clients – Community."* Being a professional services company, GIAC Enterprises prides itself on the quality of its people. GIAC strongly believes that the right people, empowered with the right solutions will always deliver the best service in the industry to its clients. As a result, GIAC has created a "gentler and kinder" consulting model to retain their resources in a very competitive labor market. This is critical because their associates are the company's major revenue producing assets. And those assets spend the majority of the time working on projects for clients in remote locations. As a result, company policy regarding travel and working from home changed significantly when GIAC broke away from its original "Big 8" parent. Now, associates travel Monday morning to Thursday evening instead of the previous model of Sunday night to Friday evening. This translates into 40% fewer nights spent away from home. On Fridays, associates can choose to work from either home or the GIAC offices. This arrangement allows many of the associates to travel to exciting destinations for "3 day weekends" where they work Friday at that remote destination via connections if necessary.

Information sharing across the GIAC Enterprise is also a critical component of its culture. As part of its "*Respect and Serve*" culture, GIAC expects its associates to share lessons learned, and account or industry information across the enterprise to deepen its total knowledge base. By sharing knowledge, GIAC's leaders believe they can continuous improve the service they provide to their clients. To facilitate this information sharing, GIAC is a heavy user of Lotus Notes.

Notes is used for email by all GIAC associates. In addition, workflow solutions such as time and expense reporting have been built in Lotus Notes. A knowledge base of engagement, client, lessons learned and other relevant topics has also been built in Notes. As a result, associates spend a great deal of time refreshing their satellite databases from the "mothership's" master databases of email and knowledge exchange.

Organization

GIAC is organized into six major divisions: Executive, R&D, Consulting, Software, Alliance Management, and Outsourcing. All the general and administrative functions (such as human resources, accounting, marketing and legal) fall under the executive division. The R&D group is a think tank of PhDs and scientists who create patent-able solutions, whether software or other intellectual property. Many of their ideas become services offerings provided by the Consulting or Software divisions.

Go to Market Strategy

The GIAC Enterprises business is not one of a simple transaction targeted at the mass consumer. It is, rather, the establishment of a trusted business partner relationship with a customer that comes from demonstration of expertise, reliability, business acumen, and empathy. Thus, "*Respect and Serve*."

GIAC Enterprises target client base is composed of companies with $500 million of revenue or greater. The targets are divided into industry segments, and account management teams are assigned to each target. The account team prospects by learning the potential client's business and looking for business problems or opportunities. As the account team builds the relationship they determine the type of solution to sell to the client: integration or custom development services, software solutions, outsourcing or alliance partner solutions.

Consulting.

If the project sold is integration or custom development work, an engagement team is formed and delivered to the client site. The engagement team is typically comprised of 30 or more associates (often numbering in the hundreds) who analyze, design and implements the solution for the client. Project work is usually priced on a deliverable product basis, but some time and materials billing does still exist.

Software.

The software segment of GIAC's business is very much like that of other software providers. GIAC markets its software through a direct marketing channel, the Web, and a small sales force. When software is sold, the client has the choice of implementing the software themselves or contracting with GIAC for professional services.

Outsourcing.

Outsourcing is a specialized business unit where GIAC assumes the operations of a client's IT infrastructure by placing its resource on site to run the operation. This is billed on a complex fee schedule dependent on service levels and other factors. GIAC is a minor player in this market but intends to grow this segment of the business. The consulting division provides this group with invaluable insight and sales leads.

Alliances.

Alliances with other IT related companies provide GIAC with an ability to serve clients even when GIAC does not have the expertise or the software solution. GIAC's alliance

program includes sharing product and client information with their certified alliance partners. This is primarily executed via electronic means.

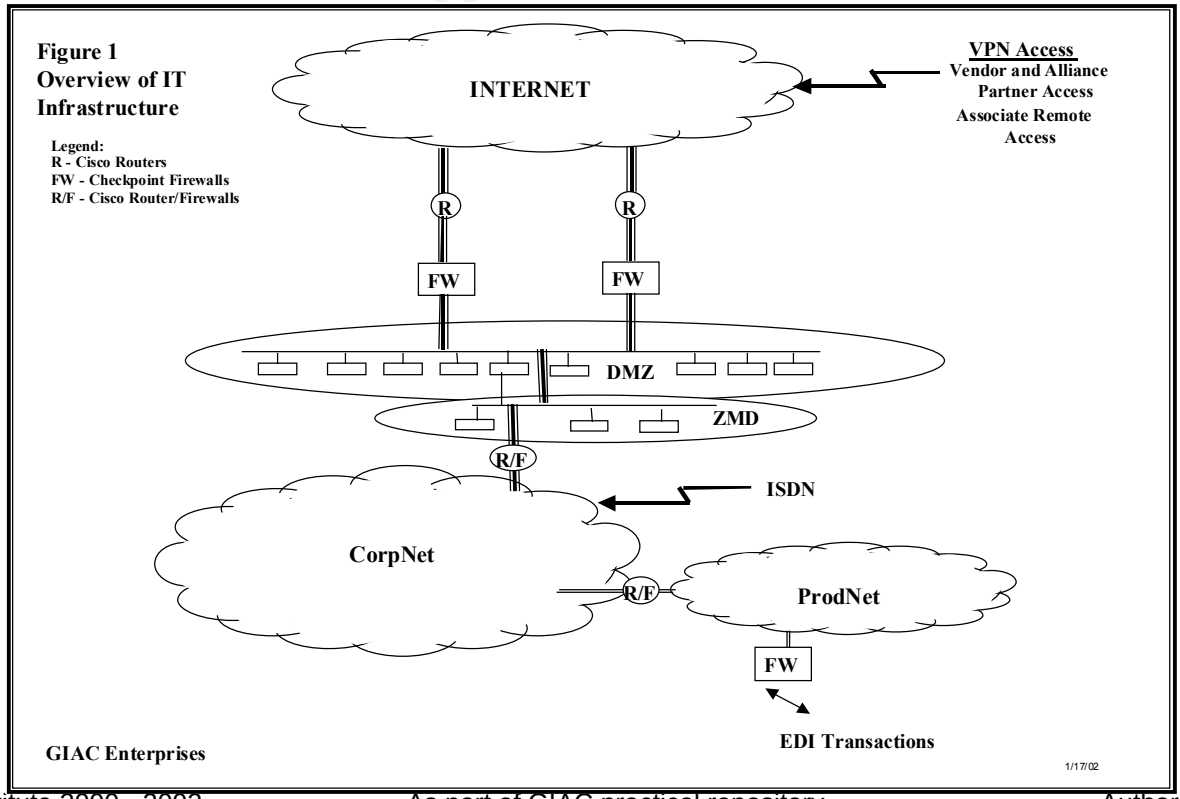
IT Infrastructure

Infrastructure Summary.

The overall infrastructure is accessed through multiple points: 1) border gateway router from the internet into a firewall protecting the Demilitarized Zone (DMZ), 2) controlled access points for GIAC associates' remote access, 3) controlled access via firewalls for alliance partners, and 4) secured firewall for Electronic Data Interchange transmissions. Figure 1 illustrates the GIAC infrastructure access points.

The GIAC network is divided into a corporate network of servers and applications and a production network of secured applications. Applications such as the general ledger, accounts payable and receivable, and select intellectual property repositories run inside the ProdNet. The corporate network is home to GIAC's other internal applications, such as the consulting division's knowledge repository, the project costing and billing system, and the alliance program databases.

Because the corporate network serves the needs of many constituents, it is sub-segmented to isolate selected servers from other servers. Alliance partner servers are isolated so users accessing the corporate network from the alliance partner gateway cannot get to other internal applications. The GIAC router/firewall network isolates this subnet. Another example of a subnet that is isolated is the ZMD. The ZMD houses servers that are necessary to complete transactions originating from the web servers in the DMZ. The design allows the DMZ web servers to access these applications and database servers, but the ZMD servers cannot be accessed directly by the external world. Figure 1 illustrates the design.



The GIAC infrastructure is protected by a defense in depth strategy. The GIAC defense includes:

- all access points having a firewall,
- critical functions are isolated and protected by router/firewalls,
- intrusion detection nodes monitoring traffic at strategic network points,
- host based intrusion detection is applied on selected machines,
- authentication and access is controlled rigorously at both the network and application level,
- anti-virus protection is applied in a multi-tier strategy, and
- databases are secured.

IT Infrastructure Walkthrough.
The architecture of the infrastructure is the responsibility of the Chief Information Officer who reports to the Chief Executive Officer. The CIO has six vice presidents who share responsibility for the implementation and execution of the architecture along with a Chief Technologist who is serves as the architect in charge. The six vice presidents can be subdivided by their functional responsibilities as:

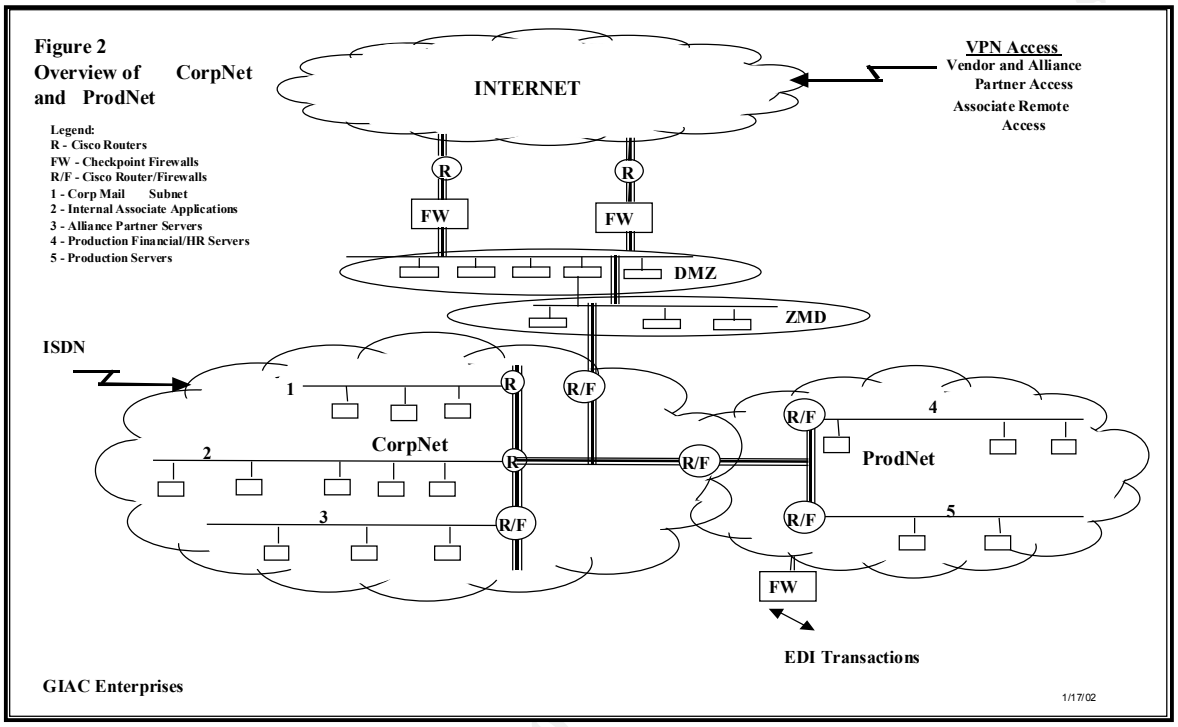
- VP, Internal Applications
- VP, Customer Applications
- VP, Operations
- VP, Network Design
- VP, Information Security
- VP, Planning and Analysis

An excellent way to understand the GIAC IT Infrastructure is to examine the role of each group.

Internal Applications.
GIAC considers the applications that reside on its internal corporate network as internal applications. These applications and databases are not intended for general public access. The internal applications are sub-segmented into separate subnets as depicted in Figure 2. Subnet 1 is the GIAC messaging subnet. Subnet 2 is the core internal applications subnet. Subnet 3 houses the alliance partner applications and databases.

As previously mentioned, GIAC runs email, workflow and knowledge exchange applications on Lotus Notes. Domino servers running in clusters of Sun Solaris E4500s provide the base for these applications. However, access to the Domino

servers depends on the function and the user. These servers are specifically represented on Figure 3 as boxes labeled A.



For Internet mail addressed to @GIAC.com, emails transit a mail relay that sits in the DMZ of the GIAC architecture. Those relays accept inbound mail, and then do Domain Name Services lookups prior to forwarding the mail to relays residing inside the ZMD. The ZMD mail relays forward the mail to the Domino servers that reside inside the CorpNet. A recent addition to the internet mail architecture is a series of Linux boxes that sit in front of the mail relays and also surround the Domino servers. These Linux boxes are hardware appliances (hardened systems with stripped down operating systems) that serve as antiviral mail filters running the signature checking software provided by McAfee, one of the leading anti-virus providers. The DMZ servers and applications are illustrated on Figure 4.

The internal applications supporting the Executive division mostly reside on IBM OS/390 architecture mainframe sitting within the ProdNet. These applications include:

- general ledger,
- accounts payable,
- accounts receivable,
- purchasing,
- fixed assets,

- human resources, and
- profitability analysis.

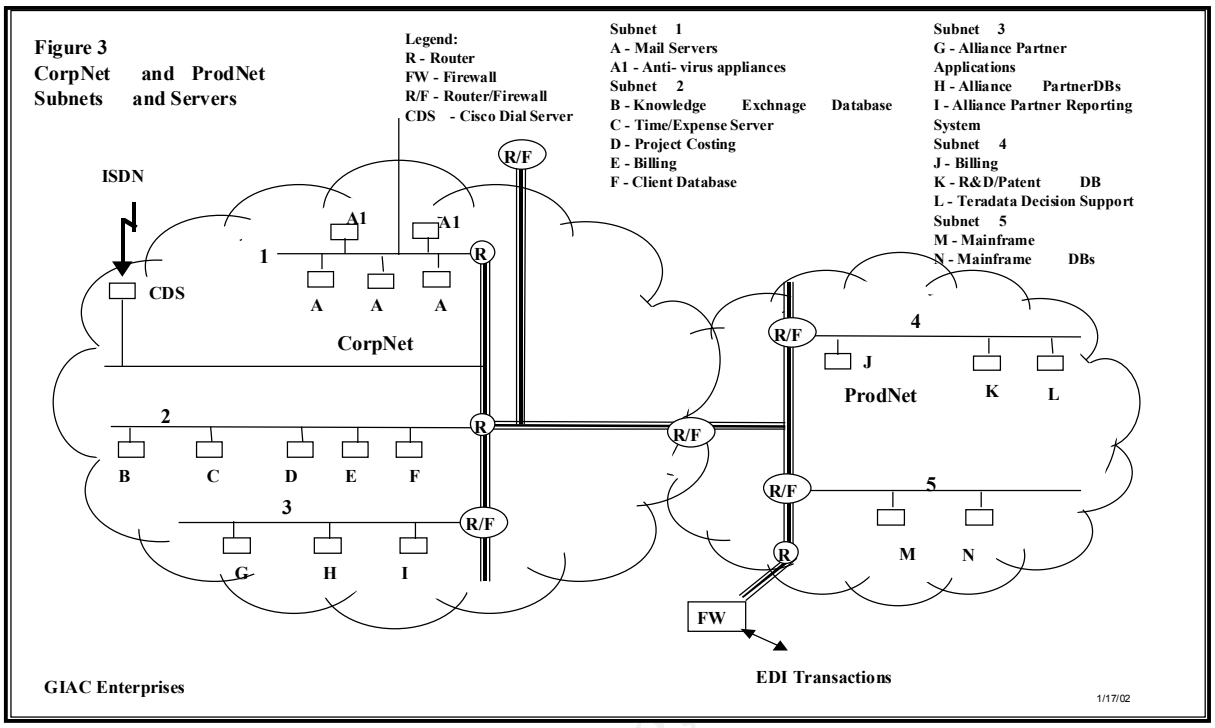
The applications are from Peoplesoft and run with DB2 as the database engine. They are represented on Figure 3 as boxes M and N that reside on subnet 5.

Also resident within the ProdNet are Unix based applications and databases that support the R&D department and legal. In addition, a decision support information warehouse running on Teradata hardware resides on subnet 4 of the ProdNet as illustrated in Figure 3 as boxes J, K and L.

Internal applications that the associates primarily use include time/expense reporting, project costing and billing, email and knowledge exchange databases. They all reside within the CorpNet. The time and expense modules are Lotus Notes workflow applications. The data is routed on the basis of rules through a review and approval chain of command. Once approved, the time and expenses are passed to the project costing system, a home grown system running on Sun Solaris 4500s, and to the ledger. From the project costing system, project managers perform analysis and prepare billings and adjustments. Those transactions move via interface to a billing module (which is also resident on the Sun Solaris 4500s) which produces invoices or credit memos, and then passes an interface file to the general ledger and accounts receivable. These applications and databases are represented on subnet 2 of Figure 3 as boxes C, D and E.

The associates replicate their email and knowledge exchange databases by connecting to the network either within the Corporate Network, or remote access. Their local databases synchronize with the master database to exchange inbound and outbound email and knowledge updates. If the email is destined for an internal address, it flows through one of the mail filters to scan for viruses and then routes within the Domino server to its destination. If the email is routed for the Internet, it passes through the mail filter, then the email is routed by the DNS services on the Domino server to an egress gateway.

In addition to Executive and Associate internal applications, a series of alliance partner applications are considered internal applications. These applications, like the other two types of internal applications, sit inside the corporate network of GIAC. They are not intended for general public access. Therefore, alliance partners access these applications through a different access path. A separate router/firewall controls the access to the alliance applications. These applications are hosted on Solaris 4500s. The relevant data is housed in Oracle databases running on clustered Sun Solaris 4500s. The applications include prospect management, contact management, product/services catalogs, and other Customer Relationship Management modules. The base applications are Siebel CRM applications. These applications are also represented on Figure 3 as residing on subnet 3.

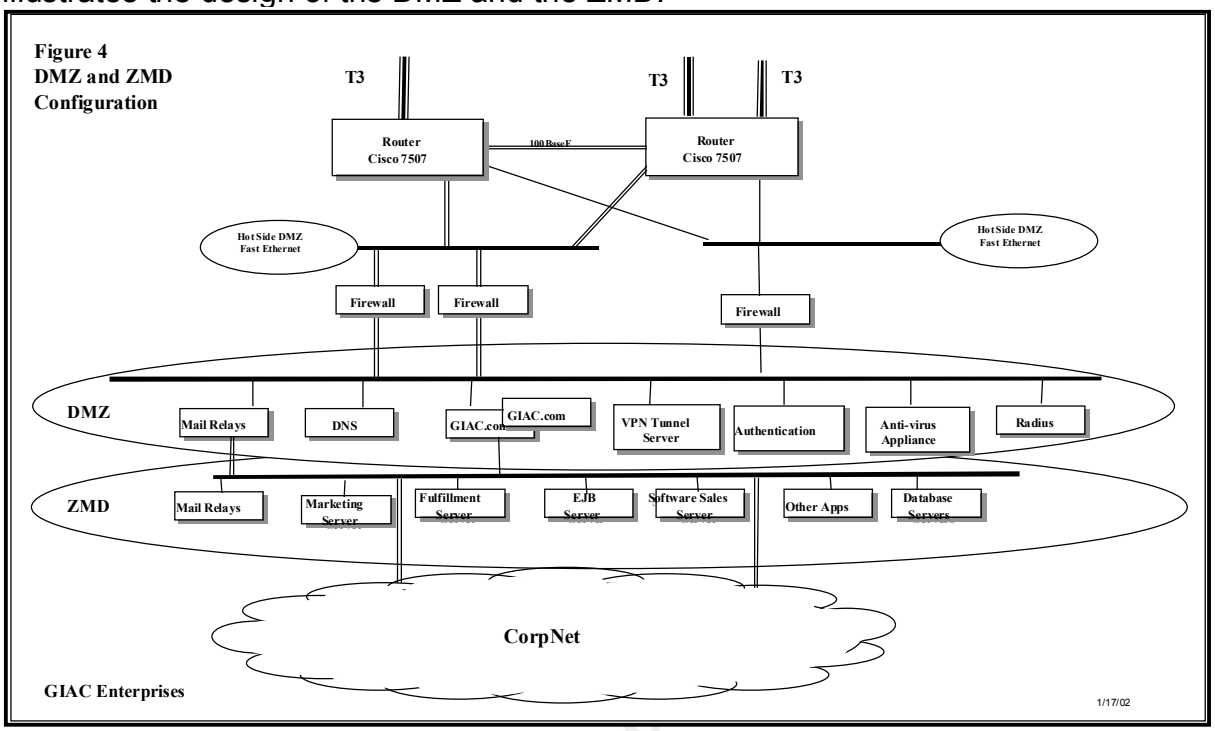


External Applications (Client Applications).

Being perceived as an innovator in the application of technology, it is important that GIAC present a technology savvy exterior to the public. As a result, GIAC senior management believes its GIAC.COM web site must project an image of technological sophistication. It must be fast and reliable as measured by the Keynote 40 standards. It must deliver value to the client in terms of the web site's functionality. Lastly, it must be secure.

In reality, the site has limited functionality in comparison to other major web sites. The GIAC web site sits behind a firewall in the Demilitarized Zone (DMZ) of the overall architecture. GIAC.com is the web site runs on Apache Servers residing on clusters of Intel based Linux operating system servers. Mostly the web site promotes the services of GIAC. Information on the types of services provided, software solutions, alliances, and other relevant information is available for review. In addition, to meet the need for value added functionality, clients can request information, inquire on account status, and order selected software products and upgrades. To perform these tasks, the web servers access applications resident on an isolated subnet. These applications are said to reside in a "ZMD." The ZMD is the mirror image of the DMZ. The servers in the ZMD are connected to the Corporate network through the cold side of the firewall, but cannot be seen in the outside world. The DMZ servers are connected to the outside world through the hot side of the firewall, but cannot be seen by the Corporate Network. The common ground between the two is where the web servers access the applications

to complete a transition such as the purchase of a software upgrade. Figure 4 illustrates the design of the DMZ and the ZMD.



Operations.

The Operations team is responsible for the production systems that reside in the DMZ, ZMD, ProdNet, and the Corporate Network. They monitor the systems for operational issues, perform the required backups and restores, administer change management processes and interface with the Network and Security groups. Figure 5 lists a summary of the GIAC Enterprises hardware inventory.

Operations, in conjunction with Information Security, is responsible for ensuring that UNIX systems deployed on CorpNet and ProdNet have safe, hardened operating systems and configurations. Protecting against all possible remote and local access attacks is a daunting challenge. Minimizing risks is the objective of the Operations and Information Security teams. For example, requiring strong passwords or disabling vulnerable services such as telnet, FTP, rlogin, rsh, HTTP, HTTPS, and SSH are critical. But, buffer overflows and other vulnerabilities "subvert even the most hardened UNIX systems…[however] it is battle that must be fought." [1]

FIGURE 5. Summary of hardware managed by Operations.

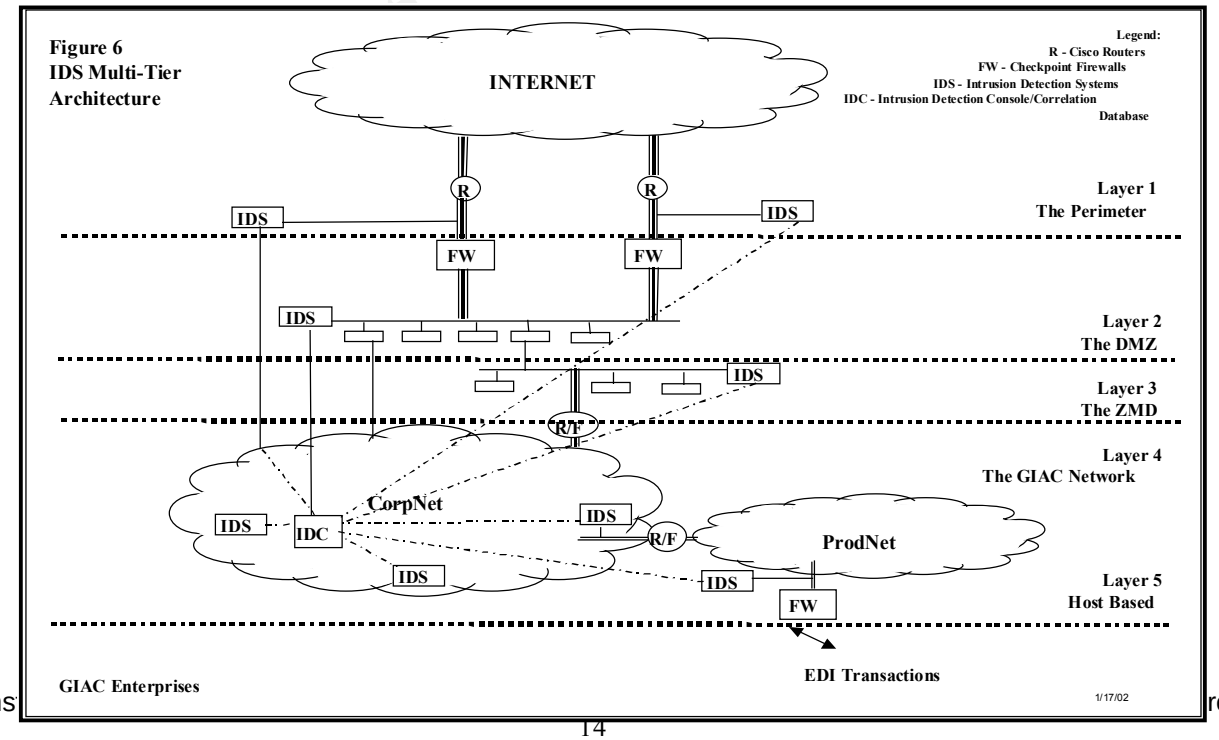
ZONE	LEGEND	MODEL	OP SYSTEM	FUNCTIONS
DMZ & ZMD	Mail relays	8 Sun 450s	Solaris 7	Send Mail
	DNS	Cluster of Sun Ultra 10s	Solaris 7	Domain Name Services

	GIAC.com	Multitude of Intel Servers – load balanced	Linux – Red Hat	Apache Web Servers
	VPN Tunnel Server	6 Intel servers	Linux – Red Hat	SSL encrypt/decrypt
	Authentication	4 Sun 450s	Solaris 7	Security
	Marketing Fulfillment Server	Cluster of Sun E4500s	Solaris 7	Database Servers
	Database Servers	Cluster of Sun E4500s	Solaris 7	Database Servers
	Software Sales	Cluster of Sun E4500s	Solaris 7	Database Servers
	Anti Virus Appliance	Intel server	Linux – Red Hat	Anti Virus Appliance
CorpNet	A	Cluster of Sun E4500s	Solaris 7	Domino Servers
	A1	Intel server	Linux – Red Hat	Anti Virus Appliance
	B	Cluster of Sun E4500s	Solaris 7	Domino Servers
	C	Cluster of Sun E4500s	Solaris 7	Time/Exp Notes Apps Servers
	D	Cluster of Sun E4500s	Solaris 7	Project Costing App Servers
	E	Cluster of Sun E4500s	Solaris 7	Billing App Server
	F	Cluster of Sun E4500s	Solaris 7	Oracle Database Servers
	G	Cluster of Sun E4500s	Solaris 7	Alliance App Servers
	H	Cluster of Sun E4500s	Solaris 7	Alliance Database servers
	I	2 Sun E4500s	Solaris 7	Alliance Reporting System
ProdNet	J	Cluster of Sun E4500s	Solaris 7	Apps and DB servers
	K	4 Sun E4500s	Solaris 7	Patent & R&D apps and data
	L	Teradata		Information

				Warehouse
	M	IBM S/390 Parallel	OS/390	Mainframe apps
	N	IBM S/390 Parallel	OS/390	Mainframe DB2 Databases

Information Security.
The GIAC information security team is responsible for the company's information security policies, compliance, associated technology, and architecture. The information security team chooses, installs and administers the firewalls protecting the perimeter of the Company. GIAC uses Checkpoint firewalls with Stateful Packet Inspection running on Nokia appliances. The advantage to GIAC of deploying SPI firewalls is "in addition to selectively allowing or denying access based on information in a packet's header, SPI firewalls keep track of the larger context, or 'state', of the specific transmission. By maintaining a table of current connections and their most recent events, these firewalls are able to spot abnormal sequences which might represent a threat." [2] This capability helps GIAC detect denial of service attacks such as SYN floods.

In addition, the security organization monitors the network with intrusion detection devices strategically placed around the network. Nodes are placed outside the firewall, and inside the corporate network at key points in a multi-tiered approach. Refer to Figure 6. The IDS sitting outside the firewall is in promiscuous mode and listens to all traffic that passes. It then forwards its data to an IDS console and repository for correlation with the internal nodes' data. GIAC has chosen to use two different IDS tools: a freeware product, SNORT, and a proprietary product from ISS. In both cases, the IDS devices are deployed as appliances sitting on the network. The appliances have stripped down, hardened configurations of hardware and operating systems. Tripwire is used as a host based intrusion detection method.



The security organization also administers authentication processes. Account setup, password management, and remote access authority come from the Security group. Security advocates the use of very strong passwords to help ensure the integrity of the network. This is necessary because most associates carry a laptop configured to access GIAC or client's infrastructures, and the laptops could be easily stolen. As a result, security requires a 7 digit password which includes at least one number and one upper case letter, and cannot be a dictionary word. Not using a dictionary word is important because 'password crackers', as Cliff Stoll noted in the The Cuckoo's Egg, "can encrypt every word in the dictionary. Make a list of encrypted English words from your dictionary. Then, it's a simple matter to compare what's in my password file to your list of encrypted passwords…[a password cracker] could find anyone's password, so long as it was an English word."[3]

Information Security uses a proprietary tool from Systor to administer GIAC's accounts in a Role Based Access Control method. The Systor system interfaces with the Unix based distributed applications and the mainframe based RACF application.

Network Design.

The network group operates a combination of network topologies to achieve GIAC's business objectives. Their responsibility covers both voice and data. The primary network is an IP network. In addition, with the mainframe, SNA also is supported. The network group selects and maintains the routers used to control the IP network. Operations installs and maintains the controllers used in the SNA network.

GIAC, like much of corporate America, is a large Cisco user. All the company's routers are Cisco routers. The routers are designed to filter traffic and limit access to and from a network sub-segment based on a series of rules. The rules are housed in Access Control Lists (ACLs). To protect the routers and their ACLs, and therefore the GIAC network as a whole, the network group must implement strong processes and procedures. For example, "difficult to guess telnet passwords, SNMP community names, limited FTP and TFTP usage, and logging for everything(and someone assigned to monitor those logs)" significantly reduces network risks.[4]

In addition, the network design team works with Operations and Security to design the overall IT infrastructure architecture. Specifically, Network Design is responsible for ensuring that the DMZ and ZMD subnets are isolated. The network team also designs the network architecture to compartmentalize applications to minimize exposure to breaches of security. An example is the isolation of alliance partner servers from other GIAC servers. Network engineers deploy a router/firewall appliance to isolate the subnets. While a router filters packets and can offer a degree of isolation to a network, the addition of firewall software greatly increases the security and resulting isolation. CISCO routers with firewall functionality are used internally to isolate subnets. Figures 2,3, and 4 illustrate where these are deployed.

The network team is also responsible for working with GIAC's ISPs and other voice/data providers to ensure reliable service. They have designed in redundancy as to the providers and adequate bandwidth to support operations. Recent terrorist events and the growing prevalence of Distributed Denial of Service attacks make this redundancy critical. Enterprises like GIAC must ensure that their business can operate if should major telecommunications carriers, such as AT&T and WorldCom are crippled during an attack according to Carlos Recalde, director of telecommunications at a major services provider.[5] In addition, enterprises must be prepared in the event their ISP provider is flooded via a DDoS or exploitation of another vulnerability such as those found in the Border Gateway Protocol.[6]

A critical component in GIAC's architecture is its remote authentication and authorization strategy. The policy is set by the security organization, but the network design team is responsible for the design and implementation of the corresponding solution. In GIAC's environment, a Virtual Private Network (VPN) is the primary method used to secure communications for associates working remotely. In addition to the IPSEC encrypted transmission that VPN provides, GIAC requires strong authentication via SecurID tokens. Alliance partners are required to connect via a VPN and are required to use tokens to provide for strong authentication. The VPN servers sit inside the DMZ and use the authentication server. Refer to Figure 4.

In addition to VPN, some associates connect from remote locations via ISDN connections. This method of connectivity is primarily used for the GIAC executive team. The Cisco dial server handles authentication on the connection of the ISDN line and services such as ANI identification are enabled to verify that the ISDN connecting is a trusted line.

Additionally, GIAC's network team is designing its wireless network strategy. As wireless technologies move deep into the mainstream, setting solid foundation and ensuring security is critical. The network team is responsible for the overall usage strategy of wireless, but the security team is responsible for defining the security-related policies. Primary plans are to combine VPN with wireless to secure the transmissions.

II. GIAC Enterprises Information Security Policies

Because of the technology services that GIAC provides its clients, it is critical that GIAC's corporate image of a technology leader not be tarnished. Therefore, GIAC has a Vice President of Information Security whose responsibilities include the assessment of risk and setting of security policies. The VP of Information Security feels that the security charter is:

> Minimize information systems related risks to the business operations of GIAC and the corporate image while providing as productive a work environment as possible.

Enabling GIAC's associates and alliance partners to work in a productive manor is a significant goal. Yet, the corporate image of GIAC must be protected. This charter is important to the setting of information security policy as seen in the assessment of risk.

Areas of Risk

Risk to GIAC Enterprises has been assessed using the OCTAVE[SM] methodology published by the Carnegie Mellon Software Engineering Institute CERT Coordination Center. The methodology framework breaks the process into three phases: understand the threat, then identify vulnerabilities and finally determine the risk.[7]

1) Access and Authentication of Remote Users.

Threat: HIGH
The threat of unauthorized users trying to access the GIAC networks to access confidential data is considered high. The threat to GIAC is that unauthorized users take advantage of the remote connection options in the network to connect and pilfer confidential information. GIAC is a publicly traded company, and access to sensitive financial information or forecasts could give someone an 'insider' advantage for the purposes of manipulating the stock market. Additionally, the professional services industry has become very competitive with the leading firms going public. Pressure to compete has increased corporate espionage. Access to GIAC's client data, knowledge base and intellectual property could be very valuable information.

Vulnerability: High
There are multiple access points into the GIAC network, which provide opportunities for the threat to manifest itself. The vulnerability increases because of the heavy dependency GIAC has on the remote access process - - - tens of thousands of associates access the network every day as do hundreds of business partners. Additionally, GIAC's thousands of laptops configured to access the network are prime targets for theft. Controlling whom, how and where people can access the GIAC network is a necessity. But it is also critical to provide an easy to use, productive environment. Enabling remote work is one major staff retention goal that is central to GIAC's '*people'* philosophies.

Risk: High
The risk to GIAC considered high because the consequences could be very serious. If an unauthorized user accessed GIAC's network for purposes of financial gain or corporate espionage, the damage would be two-fold: direct financial impact to the bottomline of the company and indirect brand image impact.

The first, direct financial impact would result from loss of revenue resulting from the compromise of intellectual property and knowledge that GIAC has developed. GIAC's competitors could use that information against them in competitive situations.

Additionally, use of confidential financial information could result in Security Exchange Commission fines and loss of market value.

The second major risk is damage to the brand image. GIAC has the leading consulting brand name in the technology services industry. Unauthorized access to its systems could severely tarnish its image as a technology leader, and ultimately impact its financial earnings.

Recommended Actions:
Remote access must be controlled via strong authentication to ensure who connects to the GIAC systems. The strong authentication will be achieved through the use of SecurId tokens. The cost to the Corporation is approximately $70 per 3 year token plus the infrastructure components necessary to operate the solution. Total costs are estimated to be $2.75 million dollars.

Additionally, Security requires 7 digit strong passwords.

2) Asset management of clients connecting to the Corporate Network.

Threat: High
Viruses and worms continue to proliferate and expose all systems to an extreme threat. To emphasis the point, the cost of a major outbreak is substantial. One estimate of the cost to businesses in lost productivity and cleanup efforts resulting from the Love Bug incident in 2000 exceeded $8.5 billion according to research firm Computer Economics. [8] Furthermore, the recent Code Red and Nimda viruses severely impacted corporate America. There is no reason to believe the threat of viruses and worms will decrease. Reported incidents over the past five years have grown dramatically as illustrated in

Figure 7
Source: CERT

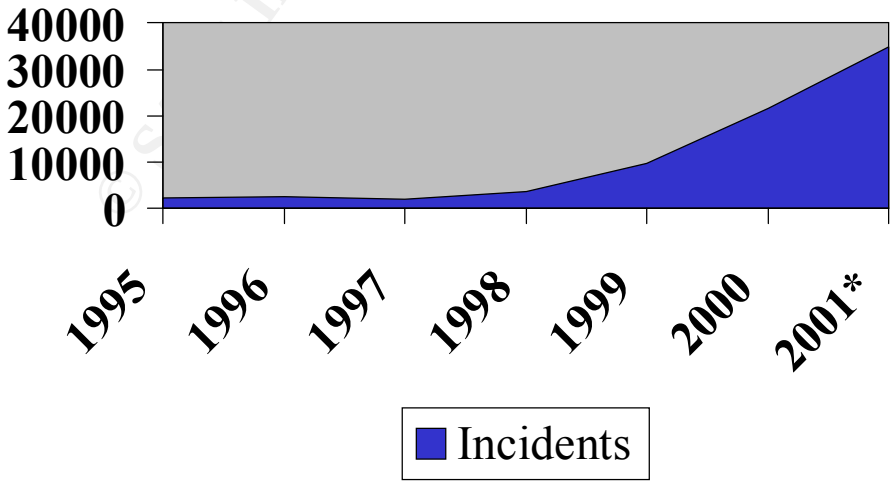


Figure 7.[9]

Vulnerability: High
GIAC is exposed to viruses in multiple ways. Computers attached directly to the network could introduce a virus in multiple ways such as through an infected diskette or through the electronic exchange of infected emails or files. Additionally, unpatched software on a computer attached to the network could be exploited (like Code Red and Nimda utilized). Devices attached directly to the network are usually under the control of a GIAC systems administrator. The Systems Administrator works to ensure the vulnerabilities are limited by requiring that security patches are applied.

A more significant risk to GIAC is the remote user. Tens of thousands of associates connect remotely everyday to exchange email, files and search the intranet and internet. The associates could try to access the network from many different points and machines. Because systems administrators are not there to oversee the devices used to connect to the network, a serious exposure exists every time an associate connects remotely.

Additionally, associates may use their computers for other personal use. For example, the prevalence of DSL and other 'Internet always-on' connections introduce new vulnerabilities to the remote use model.

Risk: High
Because associates' remote computing devices could be used for purposes other than work, and these devices are used in multiple locations such as client locations, the connectivity of these remote devices to the GIAC network is of high risk. The risk is two fold: operational and image.

Nimda and Code Red illustrated that the first threat to the business continuity is not data center operations and backup, but network integrity. If a worm compromises the network and good traffic is stuck, the business is compromised just as significantly as if the data center were offline. Remote access can introduce potentially devastating worms and viruses that could clog the network and stop business operations. To GIAC this would mean proposals could be delayed and business opportunities lost, billings delayed, internet sales lost, and vital project information not accessible on a timely basis.

The second impact of the risk is to the image of the GIAC brand. Losing a day of work to a worm or virus would severely damage the technological image of the corporation. This will result in lost revenue and market value loss.

Recommended Actions:
Pursue a policy of strong desktop standards and compliance. This will require enterprise software licenses for anti-virus software, software distribution solutions, and firewall software to validate remote users. The cost of this approach is estimated to be

approximately $1 million for enterprise McAfee rights and rights to their ePolicy Orchastrator distribution solution, plus $1 million for asset management capacity and Cygate software to verify compliance of the remote users.

However, it is important to note that anti-virus protection protects only against known signatures of viruses and worms. Anti-virus does not block the 'new' virus. So, anti-virus alone does not solve the problem.

3) Malicious attacks on the IT Infrastructure.

Threat: High
Malicious attacks on the IT infrastructure could be manifested as "cracker" attacks or DoS attacks against the GIAC IP based infrastructure. For example, malicious attacks could result in destruction of data, defacement of web sites, or the compromise of confidential data such as credit card, trade secrets, or personal employee data. The DoS attacks could be maliciously released to stop the operation of the Corporation.

Vulnerability: Med
The GIAC domain name is highly advertised, well known and is associated with a brand image of technological sophistication. Because of this, GIAC.COM site is a vulnerable commercial target for malicious attacks. Certainly, government, military and security related sites are the most targeted, but leaders in the technology industry may be the second tier of candidates.

Risk: High
The risk to GIAC's business is considered by management to be high. A denial of service attack against the GIAC web site would put a small revenue stream of software licenses and upgrades at risk for some period of time. But, more devastating would be the impact to the corporate image. Again, the image of the brand is very valuable and a malicious attack to the web site could severely tarnish the image, resulting in loss of potential revenue and severe loss of market value.

Recommended Actions:
Defense in depth strategy must be deployed including SPI Firewalls to recognize DoS attacks, IDS nodes to recognize abnormalities in traffic, network segmentation to isolate production risks, strong authentication to minimize unauthorized access, and strong policies and standards regarding systems design and maintenance standards. The cost of deploying a multi-tiered Defense in Depth strategy for GIAC is over $7 million. Firewalls being deployed and the necessary redundancy to protect the perimeter will cost approximately $500,000. Intrusion Detection Systems and monitoring will cost $1.5 million. Hardening operating systems and managing change processes will cost GIAC $1.5 million. In addition, GIAC will need to add firewalls to subdivide its network. This estimate is approximately $500,000. Deploying and maintaining hardened operating systems running on standard platforms will require considerable re-work, running from $3 million to $5 million of outlay.

Additionally, the Corporation will closely consider the strategic implications of deploying highly vulnerable operating systems within its domain. The operating systems of concern are the Windows 9x/ME, Windows 2000, Windows NT, and Windows XP operating systems.

4) Alliance Partner Access

Threat: High
The threat of unauthorized users accessing alliance program information is considered a medium threat. The majority of information exchange between GIAC and its partners occurs in various electronic forms. Product information, pricing data, as well profitability information is all stored in the alliance databases. In addition, client and prospect information is stored in the databases. As a result, important competitive information could be compromised if the alliance network were breached. However, the threat evaluation process scored this threat as medium in comparison to other threats.

However, alliance partners who are granted authorized access to the GIAC Alliance network could try to abuse their access. This threat was evaluated as being high. Having an external entity within the network poses a serious risk that someone might try to explore the GIAC network. GIAC confidential information or the GIAC infrastructure as a whole could be a target of abuse.

Vulnerability: Med
The vulnerability for unauthorized access to the alliance partner network is someone breaching the firewall which protects the access point. Firewall rules must be carefully defined to manage this risk.

Similarly, semi-trusted alliance partners who do have access to the alliance partner network might try to exploit internal network weaknesses to get to GIAC's must confidential data. These weaknesses would be network design and firewall configuration.

Risk: Med
The business risk resulting from the potential compromise of alliance partner data has been evaluated as low. Loss of alliance partner information could result in loss of revenue or even possible litigation.

The more significant risk to the GIAC business as a result of inappropriate use of the alliance partner network is the possible compromise of GIAC's most sensitive information - - - its financial results, intellectual property, and research data. Competitive espionage resulting from a semi-trusted partner could be devastating, and very embarrassing to the brand image.

Recommended Actions:
The recommendation resulting from this evaluation is to secure the alliance network with strong authentication being required for access, and very strong firewall rules managing FTP, shell utilities and other types of access. Additionally, internal firewalls must be deployed to secure the alliance partner network from other subnets within the GIAC network.

5) Encryption and Proper Security of Data

Threat: High
As a publicly traded corporation, GIAC management must frequently communicate with numerous external parties such as Board of Director members, outside legal counsel, the Securities Exchange Commission, their audit firm, GIAC's banking partners and their investment consultants. In each case, very sensitive information must be exchanged. The threat of a third party intercepting the information and using the information to the detriment of GIAC must be considered high.

Additionally, GIAC must frequently exchange confidential information with its clients. This information could be the response to a proposal, a billing, a system design or recommendation on a very sensitive issue. Such information must be protected. The threat of a third party intercepting transmissions of information to a client is considered high.

Vulnerability: High
Email transiting the public Internet could be stored and forwarded many times on its route to the final destination. Numerous opportunities exist for email to be pirated. Cellular communications can be easily eavesdropped. Faxes sent to unsecure fax machines can be picked up or read by the unintended. As a result, the method of communication used for highly sensitive information must be a secure, trusted technology.

Risk: High
The inadvertent disclosure of financial data, litigation information, or other sensitive information could be disastrous to GIAC. The damage could be financial in terms of loss of market value or fines from regulators. Or the damage could be embarrassment as the result of the leakage of sensitive information. This embarrassment can tarnish the Corporation brand and further damage the value of the Company.

A great example of this potential embarrassment is the result case of Instant Messaging conversations between two executives being posted to the Internet. The executives believed to be exchanging information and dialogue in a secure environment. The IM logs were recorded and published. The humiliation for the executives was substantial.[10]

Recommended Actions:

GIAC must set strong policy involving the use of secured communications methods. Encryption of email and encryption of attachments must be used for highly sensitive communications. Instant messaging must be banned. Cellular usage for discussion of highly confidential matters must not occur. The cost of implementing these recommendations is not excessive. The greatest expense is the training and education of the GIAC team and its support staff.

Policy

1) Remote Authentication and Access

Purpose.
This document outlines the policy for remote access. All access to GIAC Enterprises' corporate network must be via Security approved access methods. This is necessary to protect the integrity of the GIAC corporate network from unauthorized users.

Scope.
This document applies to all individuals requiring remote computing capabilities including GIAC Enterprises' associates, contract employees, alliance partners, clients, and vendors. All individuals requiring remote access must be authorized by Management responsible for the user and the request must also be approved by Information Security. All remote access is granted for a limited time period and must be renewed by Management and Information Security upon expiration.

This document applies to all remote access methods supported by GIAC Enterprises: VPN, ISDN, Alliance partner access, and vendor access.

Policy Statement.
Remote access to the GIAC Enterprises corporate network is a privilege and must be so valued by the individual using the service. This privilege is provided for business purposes only, and therefore, this connectivity may not be used for personal use. GIAC management, to ensure the appropriate use of the network, may monitor all connections.

All users of remote access must comply with strong authentication procedures (use of Tokens or PKI certificates as deemed appropriate by Information Security).

- GIAC Associates

Associates may access GIAC Enterprises through one of two methods: VPN or ISDN. Associates remote access is valid for a twelve month period and must be renewed at expiration.

- Contract Employees

Contract employees may access GIAC Enterprises only through VPN connectivity. Contract employee remote access is valid for the lesser of six months or the term of the contract.

- Alliance Partners and Vendors

Alliance partners may access GIAC Enterprises only through VPN connectivity. Alliance partner remote access is valid for the lesser of one year or the term of the alliance agreement.

Vendors may only access GIAC Enterprises on an as-needed basis. Management must authorize the connectivity and request special connectivity arrangements from Information Security. Information Security will provide special connectivity instructions and necessary accounts to the vendor. Access is granted for only one connection at a time.

- VPN Access

Information Security will provide authorized associates, contract employees and alliance partners with the necessary client software and procedural information to use VPN connections. Users of VPN will also be given tokens to ensure strong authentication upon access to the GIAC corporate network. The combination of user-id, password and tokens provides two-factor strong authentication. Additionally, the VPN client creates an encrypted SSL connection that protects data in transit.

- ISDN Access

For individuals needing ISDN connections to GIAC Enterprises, Information Security will provide authorized individuals with the modem, configuration information and accounts to make a successful ISDN connection. Individuals using ISDN will also be given tokens to ensure strong authentication upon access to the GIAC corporate network. The combination of user-id, password and tokens provides two – factor strong authentication.

Responsibility.

- Individuals using the remote access provided to GIAC Enterprises are responsible for all activity performed under their user id.

- Individuals using the remote access privileges must provide for a secure work environment by abiding by the Desktop Management policy, Password Management policy and the Encryption of Data policy.

- Management is responsible for the review and approval of requests for remote access.

- Management is responsible for the timely notification to Information Security of any individuals who terminate working relationships with GIAC Enterprises prior to the expiration of their remote access privileges.

- Information Security is responsible for the maintaining and monitoring of connectivity logs of all remote users.

Action.

For GIAC associates, failure to comply with this policy will result in disciplinary actions up to and including termination. The GIAC Enterprises' Employee Relations Board will

decide disciplinary actions, with consultation from Information Security and management.

For vendors, alliance partners, and contractors, failure to comply with this policy will result in immediate denial of access privileges. The incident will be referred to the sponsoring management for further disciplinary actions up to and including termination of contracts.

Procedures.
The following procedures are related to this policy:

- VPN installation and usage.
- ISDN usage.
- Token procurement and usage.
- Password procedures.
- Encrypting email.
- Encrypting attachments.
- Encrypting files.

2) Desktop Management

Purpose.
This document outlines the policy for desktop management. All GIAC Enterprises desktop computing devices must comply with this policy statement to protect the integrity of the GIAC corporate network from viruses, worms and other forms of virulent programs.

Scope.
This document applies to personal computers connecting to the GIAC corporate network including computers provided by GIAC Enterprises, and computers provided by contract employees, alliance partners, clients, and vendors. This document also applies to all personal computers remotely accessing GIAC Enterprises corporate network.

Policy Statement.
The GIAC Enterprises corporate network houses the computing infrastructure necessary to enable the operations of the business. As a result, threats such as virulent programs must be minimized by requiring all devices connecting to the GIAC corporate network to comply with the following policy statements:

- Hardware Configuration for GIAC Enterprises Personal Computers

All of GIAC's personal computers must be procured by complying with the Personal Computer Procurement Policy. This policy controls the models and base hardware configurations of personal computers that may be procured by GIAC. Furthermore, that policy specifies the procedures in placing orders to approved vendors.

- System Images

All of GIAC's personal computers will ship with a base system configuration designed by GIAC, but applied by the fulfillment vendor. System images will include:

  - Operating system
  - Browser
  - Email Client
  - Anti Virus Software
  - Personal Firewall software (for selected models)
  - Configuration files
  - Print drivers
  - Standard office productivity tools (spreadsheet, word processor and presentation maker)
  - LAN software (file/print services)
  - 3270 emulation software
  - VPN client software (as appropriate)
  - Desktop management agents, and

- Assorted utilities.

The listing of specific vendors and products loaded to the software images is available from the Desktop Management Design Team.

- Desktop Management System

The GIAC Enterprises desktop management system includes the agents residing on each personal computer connecting to the network and a series of servers that administer the desktop and security standards. The desktop management agents provide critical inventory management data to the desktop management system. Additionally, the agents are used to update the personal computer with any new releases of software, software patches, and upgrades. End users must not disable the desktop management agents for any reason

Desktop management agents will be polled on each connection to the network to ensure that the connecting device is current with respect to baseline corporate standards and security standards. If a device is out of compliance with security standards, the desktop management system will not allow the device to connect to the network until it has been returned to a compliant state.

- Vendor, contractor, and Associates' personal equipment

Personal computers will only be allowed to connect to the network if they comply with security standards.

- Security standards

The security standards for desktop management apply to all devices connecting to the GIAC corporate network. The security standards include:

- Having the current anti-virus engine and .dat file of approved vendors loaded and enabled
- Having an approved personal firewall system installed and enabled for remote computing devices
- Current VPN client software (as appropriate) and
- Selected other current software versions as defined by Information Security.

Information security may require selected security patches for software such as a browser or email client be loaded prior to connection. The desktop management system will enforce this according to the rules set by Information Security.

Responsibility.

- The desktop management design team is responsible for the creation and maintenance of system images. Information Security will review and test the system images for security exposures prior to release.

- Procurement will receive the system image from the desktop management design team for each approved model and configuration of personal computers. In turn, Procurement will provide the images to each certified fulfillment vendor. Procurement will be responsible for reporting on vendor performance with respect to installation of the system images.

- Information security is responsible for setting security standards related to desktop management and providing those standards to the desktop management team for enforcement via the desktop management system.

- The desktop management team administers the desktop management system. This system enforces corporate software and security standards by requiring compliance with the corporate software and security standards prior permitting connection to the network.

Action.
For GIAC associates, failure to comply with this policy will result in disciplinary actions up to and including termination. The GIAC Enterprises' Employee Relations Board will decide disciplinary actions, with consultation from Desktop management, Information Security and management.

For vendors, alliance partners and contractors, failure to comply will result in immediate revocation of network privileges. The incident will be forwarded to the sponsoring management for consideration of additional disciplinary actions up to and including termination of contracts.

Procedures.
The following procedures are related to this policy:

- Anti-Virus Software.
- Personal Firewall.
- Desktop management agents.
- Desktop management services.

3) Encryption of Privileged and Confidential Data for Exchange Via Email and Attachments

Purpose.
This document outlines the policy for encryption of privileged and confidential data exchanged by email. The pervasive use of email as a communications tool both internal to GIAC and from GIAC to the external world requires that a secure form of email be provided for the exchange of privileged and confidential data.

Scope.
This document applies to the encryption of privileged and confidential email and attachments sent by any GIAC associate. This applies to emails sent within the GIAC email domain and external to the GIAC email domain.

Policy Statement.
All privileged and confidential data must be encrypted when being sent by email. This applies to the email text and attachments if either contains privileged and confidential data.

Privileged and Confidential data is defined by the Corporate Information Classification Policy as the highest two levels of information classification encompassing both:

- Privileged Data – information protected under the attorney-client privilege
- Confidential Data – information of value to competitors, related to litigation, of regulatory nature, and associates' personnel data (salary, social security numbers, health records, etc).

Responsibility.

- Information security, in conjunction with the corporate security department, is responsible for the maintenance of the Corporate Information Classification Policy and definition of confidential data.

- Information security is responsible for the selection of approved encryption tools, methods and services.

- The GIAC Enterprises email group is responsible for the deployment of encryption tools as needed.

- All GIAC associates are responsible for understanding the Corporate Information Classification Policy and determining when confidential data is being transmitted. If the individual associate's personal computer has not already been enabled with encryption tools, the associate must request the tools.

- Management is responsible for the review and approval of individual requests for encryption tools.

- The desktop management team is responsible for assuring patches, upgrades and new versions of the encryption tools are deployed to the appropriate clients.

Action.
Failure to comply with this policy will result in disciplinary actions up to and including termination. The GIAC Enterprises' Employee Relations Board will decide disciplinary actions, with consultation from Information Security and management.

Procedures.
The following procedures are related to this policy:

- Encrypting email.
- Encrypting attachments.
- Encrypting files.
- Install of encryption software.

III. GIAC Enterprises Information Security Procedures

Desktop Management Procedures: Anti-Virus Software

Purpose.
This document outlines the procedures for configuring and administering anti-virus software on the desktop.

Related Policy.
Desktop Management.

Procedures.

PROCEDURES	RESPONSIBLE PARTY
1) Administration	
Anti-virus software is selected and certified by the Information Security group. Why: Critical to have certified anti-virus vendor(s) and product(s) upon which GIAC can rely. When: Anti-virus vendor selection is awarded on a three-year cycle. It is expensive to change vendors and products more frequently.	**Information Security team** Measurement: Measured by the timely renewal of contracts with the anti-virus provider(s).
The software is distributed on all new personal computers procured by GIAC Enterprises via the corporate system image. Why: It is critical to have every GIAC desktop with anti-virus protection. Every desktop is potential entry point for virulent programs. Therefore, every desktop needs to be protected. Installing the anti-virus on the new desktops as procured makes sure each one has the software from the beginning of its useful life at GIAC.	**Desktop management team** Measurement: Metrics is tracked of machines that do not have the software installed. The vendor Service Level Agreement is that 100% of new machines will have the GIAC anti-virus software installed. As the desktop management system identifies PCs that do not have the anti-virus software, the metrics measuring this SLA is updated.

When: The anti-virus software and configuration is provided to the fulfillment vendors for installation with the system image.	
If anti-virus software is not on a GIAC Enterprises personal computer, the software should be obtained from the desktop management web-site. The URL is: home.giac.com/desktop/antivirus/. The desktop management system will record the requester, reason for the request, and execute the download. Open the downloaded installer and it will install and configure the software correctly. Why: It is critical every PC is protected. If an error has occurred and a PC on the corporate network does not have the certified anti-virus software, it must be reported and loaded. When: This procedure should be followed immediately upon recognition that the software is missing.	**Desktop management team.** Measurement: All requests for download are tracked by the desktop management system. Metrics on the number of requests, reasons for requests and mean time to respond are tracked. Follow-ups to verify successful installation of the software is performed by the desktop management system and tracked.
If a vendor, alliance partner or contractor's personal computer does not have an approved, current version of an anti-virus program, management may request anti-virus software for them from the desktop management team by accessing the desktop management website. The URL is: home.giac.com/desktop/antivirus/. Again, the desktop management system will record the requester, reason for the request, and execute the download. The installer downloaded will install the software and configure the software correctly. Why: It is critical every PC connecting toe the GIAC corporate network be protected.	**End user management requests software** **Desktop management team operates the desktop management system.** Measurement: All requests for download are tracked by the desktop management system. Metrics on the number of requests, reasons for requests and mean time to respond are tracked. Follow-ups to verify successful installation of the software is performed by the desktop management system and tracked. Devices that fail to comply will not be connected to the network.

If a vendor or partner does not have appropriate protection, they must load certified anti-virus software prior to being allowed to connect to the network. When: This procedure should be followed immediately upon recognition that the software is missing.	
2) Configuration.	
The anti-virus software on the client will be enabled to automatically scan the hard drives of personal computers when the computer is turned on. Why: Each hard drive must be scanned on boot up of the personal computer to establish a trusted environment. This verifies that viruses and worms are not resident at the being of a session. When: This procedure is executed every time the machine is turned on or restarted.	**Information Security team configures the software for the system image.** **Desktop management team implements.** Measurement: The ePO system verifies that the configuration of the anti-virus software is accurate and the scanning is enabled. If not, it forces adjustment to the configuration and reports to the desktop management system.
The anti-virus software will be configured to scan any diskette inserted in the personal computer. Why: Diskettes can pass viruses and worms. Each diskette should be scanned. When: This procedure is executed every time the diskette drive is activated with the insertion of a diskette.	**Information Security team configures the software for the system image.** **Desktop management team implements.** Measurement: The ePO system verifies that the configuration of the anti-virus software is accurate and that diskette scanning is enabled. If not, it forces adjustment to the configuration and reports to the desktop management system.
The anti-virus software will be configured to scan any imported or downloaded files. Why: Files downloaded, FTP'd, and attachments detached or otherwise	**Information Security team configures the software for the system image.** Measurement: The ePO system verifies that the configuration of the anti-virus

imported can include a virus or worm. Therefore, the anti-virus will scan each new file as imported or downloaded. When: This procedure is executed every time a file is being saved to disk through the import, download via browser, FTP, or detach attachment functions.	software is accurate and that diskette scanning is enabled. If not, it forces adjustment to the configuration and reports to the desktop management system.
The configuration of the anti-virus software will not be modifiable by the end user. Only the desktop management team may change or disable the anti-virus software. Why: Disabling or changing the configuration of the desktop anti-virus software increases the exposure to company. Viruses can be introduced while the anti-virus is disabled. When: At all times.	**Desktop Management team** Measurement: The ePO system verifies that the configuration of the anti-virus software is accurate and the anti-virus software is enabled. If not, it forces adjustment to the configuration and reports to the desktop management system. Notification goes to the desktop owner and their management of violation of anti-virus policy and procedures.
End users are not authorized to turn off or disable the anti-virus software. Why: Disabling or changing the configuration of the desktop anti-virus software increases the exposure to company. Viruses can be introduced while the anti-virus is disabled. When: At all times.	**Desktop Management team** Measurement: Notification goes to the desktop owner and their management of violation of anti-virus policy and procedures.
The anti-virus software will be configured to automatically look for new engine upgrades or new .dat files on start up. Why: Anti-virus software only protects against known strains of viruses and worms. Therefore, it is important to keep the software as current as possible. The GIAC vendor(s) of choice provide frequent updates to the software and its supporting	**Information Security team configures the software for the system image. Information security team works with vendor(s) to ensure updates are available on a timely basis.** Measurement: Download penetration reports will be tracked by upgrade or new .dat file to track the penetration to 100%.

recognition or signature files. When: Each time the PC is booted or restarted, a query will be made to see if new engines or ,dat files are available.	
The anti-virus software will be configured to report any incidents (identification of viruses and subsequent action) to a central anti-virus incident repository. Why: As the software catches intrusive viruses and worms, it is important that information regarding what is being captured be shared with Information Security. Information security can look for patterns, types of viruses, and other relevant information. Information security can then take further action if warranted. When: Each time the PC identifies a virus and the eradication or fix process is concluded the anti-virus software will log the incident. On the next start-up, the logs are forwarded to the central repository.	**Information Security team configures the software for the system image.** Measurement: Incidents are reported daily and a daily incident management report is generated from the desktop management system. The manager of the desktop management team and the manager of the information security team review this report.
3) Compliance.	
The desktop management team is responsible for ensuring the client level compliance with the Desktop Management policy via this procedure. Why: Desktop management involves the inventory of equipment, license management, and configuration management of the GIAC PCs. Anti-virus is one of many software solutions operating on the PC. Therefore, the desktop management team is responsible for the anti-virus software compliance as they are for compliance with other desktop standards.	**Desktop management team** Measurement: Reports will be generated daily.

When: At all times.	
Anti-virus compliance servers will be maintained with current configuration rules and all clients must be authorized against the servers' configuration rules prior to connections being established. Why: Configuration standards for the anti-virus software are critical to the protection of GIAC's corporate network. As the software changes, configurations may need to be modified. Information security is responsible for the configuration standards of anti-virus software. When: At all times.	**Information Security team** Measurement: Connection logs will be monitored to ensure every connection has validated the anti-virus status and configuration on connection.
Compliance reports will be generated daily, reviewed, and signed off by the manager of desktop management systems. These reports will detail: • **Number of failures to connect due to anti-virus compliance failures** • **Number of downloads of engine/.dat files** • **Number of personal computers detected as being out of compliance and the reason code (disabled, not TSR, etc)** Why: Measuring compliance is critical to ensuring that policy is being followed. When: Daily.	**Desktop Management team produces reports.** Measurement: Manager of the desktop management systems must review and sign off on the daily reports.

FOOTNOTES

[1] Stuart McClure, Joel Scambray and George Kurtz. Hacking Exposed: Network Security Secrets and Solutions. Third Edition. Berkeley: Osborne/McGraw Hill Companies, 2001. p. 385.

[2] Jeff Crume. Inside Internet Security, What Hackers Don't Want You to Know. Harlow: Addison Wesley, 2000, p. 75.

[3] Cliff Stoll. The Cuckoo's Egg. New York: Simon & Schuster, Inc. 1990, p. 308.

[4] McClure, Scambray and Kurtz, Hacking Exposed, p. 455.

[5] Rutrell Yasin, Mitch Wagner, and Margie Semilof. "IT Managers Look for Safety, Efficiency." Internet Week. December 17, 2001(2001): p. 39.

[6] Rutrell Yasin. "Latest Hacker Target: Routers."Internet Week. December 17, 2001 (2001): p. 9.

[7] Christopher Alberts, Sandra Behrens, Richard Pethia, and William Wilson. Operationally Critical Threat Asset, and Vulnerability Evaluation (OCTAVE). Pittsburgh: Carnegie Mellon University. 1999: p.3.

[8] Larry Greenemeier. "Demand for Security Services Rises." InformationWeek. Dec. 24 –31, 2001 (2001): pp. 42-43.

[9] CERT Coordination Center. "CERT/CC Statistics 1988-2001." Carnegie Mellon University. January 10, 2002. URL: http://www.cert.org/stats/cert_stats.html, (January 12, 2002).

[10] Paul Festa. "Company Crippled Over alleged ICQ Leaks." ZDNET News. March 15, 2001. URL: http://www.zdnet.com/zdnn/stories/news/0,4586,5079593,00.html (January 6, 2002).