Global Information Assurance Certification Paper

Securing an Infrastructure with Windows 2000 and Active Directory

Brandon Lowther

GIAC-GCWN Practical Assignment

Option 1 – Design a Secure Windows 2000 Infrastructure

Version 3.1 (Revised April 8, 2002)

Abstract

Windows 2000 is a network operating system that supports a broad range of IT functional and security needs. Windows 2000 can be used to authenticate all users on a network, provide file sharing and print services, provide remote access capabilities, and support many other needs required by today's organizations. This document describes how one company, GIAC Enterprises or GE, implemented Windows 2000 and its directory service, Active Directory. The company uses Windows 2000 to perform functions such as managing users, providing connectivity between remote sites, and controlling security configurations on servers and workstations.

The first section of this document describes GE's network design and implementation. This section describes key aspects of the logical and physical topology of the network as well as some of the important security controls that are in place. The second section presents how GE implemented Active Directory. Important Active Directory elements such as name resolution, replication, as well as user groups and organizational units are discussed here. The next section describes various Group Policies implemented in the environment. Group Policy is an important element of Active Directory and allows for centralized management of a variety of functional and security parameters on all hosts in the directory. Finally, GE has security needs that cannot be solely addressed through technical means such as hardening servers or implementing additional Group Policies. The last section describes some of the processes implemented by the company that help to achieve various security objectives.

Table of Contents

Overview of GIAC Enterprises 1
GE Network Design and Implementation 2
  Overview 2
  Hardware Considerations 3
  Internet Connectivity 4
  DMZ Segment 5
  Internal Network 8
  Blacksburg Call Center Segment 10
Active Directory Design: ge.dmz 10
Active Directory Design: ge.corp 11
  Domain Name Service (DNS) 12
  Operations Masters and Global Catalog Servers 13
  Sites and Replication 14
  Organizational Units 15
  Important Groups and Delegation of Authority 19
Group Policy and Security 21
  Domain Group Policy 21
  Domain Controller Group Policy 23
  General User Policy 27
  Workstation Security Policy 29
  General Server Security Policy 31
Other GIAC Enterprises Information Security Initiatives 32
Appendix A: GIAC Enterprises Network Environment 35
Appendix B: Active Directory Environment 36
Works Cited 37

Overview of GIAC Enterprises

GIAC Enterprises (GE) is a small software development and application service provider. GE develops software that facilitates product ordering, fulfillment, and billing. GE's software product, EasyOrder, allows customers to place orders for products over the Internet. The product has several modules, including one supporting customer call centers that receive customer orders by phone. EasyOrder is a web-enabled application, uses IIS as an application server and SQL Server as its database.

EasyOrder provides two primary revenue streams for the company. First, GE sells the product to merchants who desire a turnkey solution to sell their products. These merchants install, configure, manage, and administer EasyOrder internally, although GE does provide some consultative services. Second, the company offers online ordering and billing for those companies that desire to outsource these services. Presently, one company has outsourced this function to GE. The LED Corporation sells hundreds of products on television, such as carpet cleaner, food processors, and automotive scratch removal creams. LED's customers can order products on the Internet at the GreatProducts web site (www.great-products.com) through the EasyOrder application. Alternatively, customers may place their order with a customer service representative. GE maintains a call center with customer service representatives trained to place orders for LED's products.

GE employs approximately 500 people and operates from two locations. The company's main location is in Hampton, Virginia. The majority of the company's operations occur in the Hampton office. These departments operate from this location: Accounting and Finance, Sales and Marketing, Human Resources, as well as Research and Development (software development, quality assurance, and product support). GE's customer call center is located in Blacksburg, Virginia, where it can employ cheap but competent college labor to process orders for LED Corp. Currently, approximately 100 people work at the call center.

Remote connectivity to GE networks is an important business requirement. The traveling sales force, product consultants, and company executives all require remote access capability. Remote access to GE is permitted through dial-in or by establishing a virtual private network (VPN) from the Internet. Approximately 75 people are permitted to remotely access the GE network.

The EasyOrder product is in a competitive segment of its market. The product currently enjoys several competitive advantages including its attractive user interface, security features, stable architecture, and performance. Management considers the unauthorized disclosure of product data, pricing, or software code a significant business risk. In addition, it is critical for the company to maintain its current relationship with LED Corp., and attract additional business opportunities through the outsourcing channel. Thus, it is imperative for GE to ensure the confidentiality and integrity of customer transactions and data, while ensuring the web site is continuously available

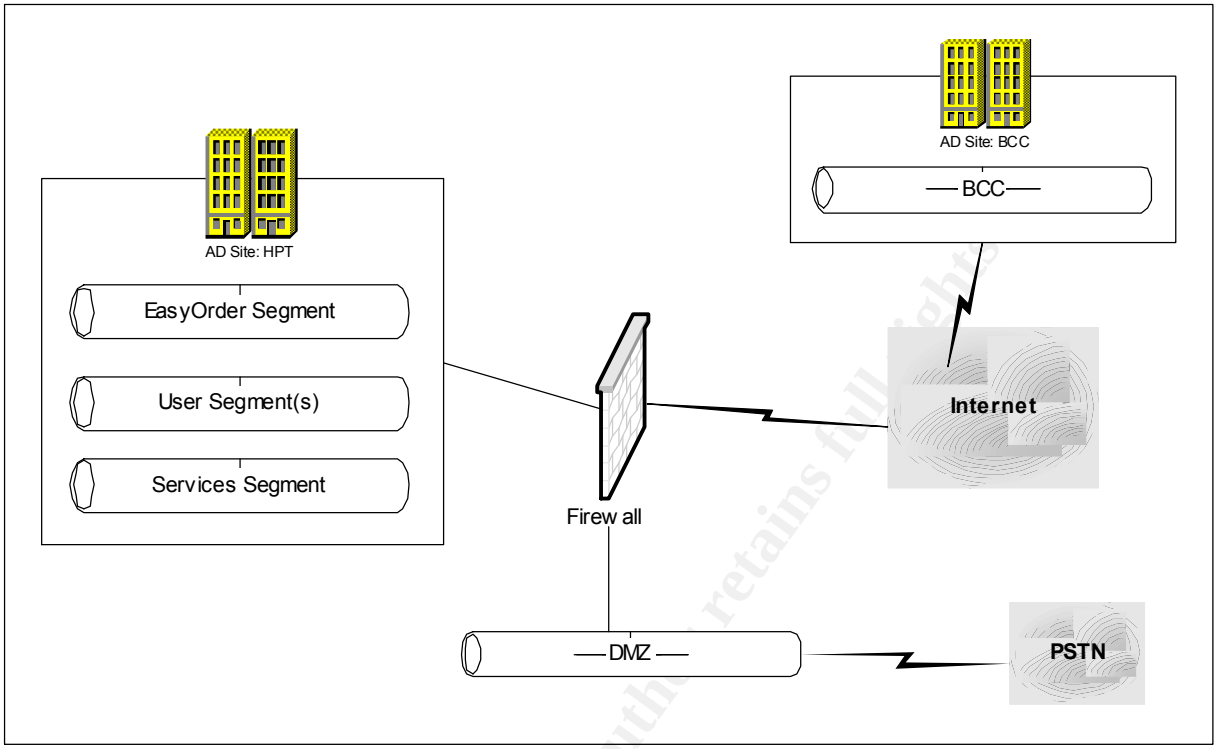
for LED's customers. In the current market environment, the company cannot afford a security incident that could damage its reputation or lead to costly litigation.

GE Network Design and Implementation

Overview

GIAC Enterprises's network consists of three primary networks. The Demilitarized Zone (DMZ) and the internal network are physically located in the Hampton office. The third segment, for the Blacksburg Call Center (BCC), is physically located in Blacksburg, Virginia. The two physical locations are configured as two Active Directory sites. Connectivity between the Hampton office and the BCC is achieved through a VPN connection over the Internet. The network speed connecting the various devices on each segment is either gigabit or 100-megabit Ethernet. A high-level overview of GE's network is presented in Figure 1. A more detailed view of the network is presented in Appendix A. Note: GE's network consists of other segments (e.g., separate segments exist for the software development and quality assurance teams), network devices, and hosts not depicted here. The diagrams presented here are intended to illustrate GE's network topology and security infrastructure, not provide a comprehensive view of all elements of the network. In addition, GE has implemented a variety of physical security controls to protect the company's assets that are not fully discussed here. Computer rooms are protected by physical access controls and access to these rooms is restricted to a minimal number of trusted administrators. Environmental controls, fire suppression, and monitoring/alerting systems are also in place. One can assume the company's physical security controls adequately protect networks and systems from theft, sabotage, and improper access to local consoles, as well as other physical threats.

GIAC Enterprises Network Overview



Hardware Considerations

GE is committed to ensuring applications and data are continuously available to users and customers. Therefore, the company uses quality hardware components from a single, reputable manufacturer. Service contracts are in place that adequately address GE's hardware servicing and replacement needs. One can assume that each server has adequate processing and memory resources to support its role in the infrastructure. The points below describe some aspects of the hardware configuration on various GE servers used to help ensure strong performance and availability.

- Disks on production servers are SCSI for optimal performance. GE uses hardware solutions to deploy RAID arrays whenever possible.

- All servers have the operating system loaded on a dedicated disk partition. This partition is separate from any partitions housing databases, websites, roaming profiles, user data, etc.

- The paging file is appropriately sized to be just larger than the amount of physical memory. On many servers, the paging file is split across one or more separate physical disks.

- Disks on file servers storing company data, user files, and user profiles are configured in RAID 5 arrays for fault tolerance.

- GE used the Active Directory Sizer tool from Microsoft to help determine the hardware requirements for its domain controllers. These servers have separate system and log disks that are mirrored (RAID 1 configuration). The AD database resides on separate disks in a fault tolerant (RAID0+1) configuration.

- The databases supporting the online EasyOrder application reside on striped (RAID 0) partitions to increase performance.

- GE used the Exchange 2000 sizing tool (Microsoft Q328745) to help define the hardware requirements for its email system. Transactional tracking log files and database files are on separate physical disks with fault tolerant partitions.

Internet Connectivity

GE has redundant network connections through different service providers at both physical locations. Maintaining Internet connectivity between the two sites is critical for servicing LED's customers. One can assume all reasonable measures to ensure the performance and availability of Internet connectivity have been taken and that bandwidth is adequate to support operations.

Two network devices reside between the Internet and the segments maintained by GE in the Hampton office. The border router and firewall filter and control the network traffic and connections to GE networks. These devices provide the first layer of security.

Border Router

GE uses a Cisco router to connect the Hampton office to the Internet. The specific hardware characteristics of the router (e.g., model, IOS version, line speed, etc.) are not relevant to this description of the network architecture. The border router is the first device where GE filters inbound and outbound Internet traffic. GE has implemented a general ACL on the router that applies to all traffic. Traffic is filtered more granularly at the firewall. The ACLs configured on the router protect primarily against IP spoofing and denial of service attacks. For example, GE does not permit packets from the Internet to enter the network if the packet has a source address of a host in the DMZ. Several groups recommend implementing these types of ACLs on Internet border routers. Failure to implement such rules has been noted by the SANS Institute as a top vulnerability in the past (The SANS Institute, "Top Twenty Vulnerabilities"). The National Security Agency (NSA) also recommends implementing ACLs similar to those implemented by GE in the NSA/SNAC Router Security Configuration Guide.

Firewall

GE uses a Cisco PIX firewall to filter and control traffic to the Internet, DMZ, and internal network segments. The specific hardware characteristics of the firewall (e.g., model,

IOS version, line speed, etc.) are not relevant to this description of the network architecture. The firewall has three network interfaces. One interface is connected to the router; the other interfaces are connected to the DMZ and internal network. The firewall performs Network Address Translation (NAT) between the internal network segments and the Internet. This helps hide the internal characteristics of the network and allows GE to use private IP addressing on the internal segment.

The rulebase on the firewall is explicitly defined to protect network segments from external and internal attacks. All packets are dropped unless permitted by a firewall rule. Example rules from the rulebase are listed below.

- Inbound connections to the IIS servers are permitted on ports 80 and 443 only.
- The IIS servers are permitted to connect to the LED Corp. customer databases only on specific ports used by the application.
- Queries to external DNS servers are permitted only on UDP port 53 only.
- The external mail server is permitted to connect to the internal mail server on port 25 only.

DMZ Segment

The DMZ Segment isolates GE's public Internet presence from the internal network. The firewall permits a limited number and type of connections to be made from Internet hosts to DMZ hosts. The DMZ contains the web servers for GE's company website, the web site customers use for ordering LED's products, as well as hosts supporting the company's network and communications infrastructure. Each host in the DMZ is assigned a public IP address.

All hosts in the DMZ are in an Active Directory (AD) domain, "ge.dmz." This domain exists to more effectively and efficiently manage host configuration. Redundant domain controllers exist that host AD integrated DNS zones for only the domain. GE diligently monitors several web sites and email lists to identify new vulnerabilities that could affect corporate hosts. Group policies are used to enforce hardening recommendations developed by the NSA, Center for Internet Security, as well as the SANS Institute. One can assume operating system and application patch levels are current and that all appropriate measures have been implemented to secure hosts in the DMZ.

Specific hosts or network services in the DMZ are discussed below.

Network Time

Maintaining accurate time is important for GE. In addition to the time synchronization requirements imposed by the Kerberos authentication protocol, the company must ensure transactions executed on the web site are accurately time stamped. Because of

the need to accurately time stamp transactions, GE does not use the Windows Time service (W32Time) to synchronize the clocks on all hosts. W32Time uses the Simple Network Time Protocol (SNTP) and meets the requirement of "loose synchronization." This protocol ensures only that time in an enterprise is synchronized within 20 seconds. Microsoft (Green and Brandolini) and RFC1769 (Mills) suggest SNTP, and thus W32Time, may be insufficient to meet the needs of companies that require strict time synchronization. Management determined that the importance of accurate time keeping required a non-Microsoft NTP solution. One can assume GE has securely implemented a time synchronization infrastructure, the clocks on Active Directory hosts are adequately synchronized, and that transactions are accurately time stamped.

Electronic Mail

GE's email system is Exchange 2000. The external mail server forwards email from internal users to the Internet and relays messages received from the Internet to the internal mail server. Email is an essential mode of communication; however, the medium presents several security risks to the company. Email can introduce viruses or worms into the environment, be used in social engineering attacks, or be used to send unsolicited mail (i.e., spam) to others. To help mitigate these risks, both mail servers are configured with antivirus and content filtering software. All inbound email and email attachments are scanned (and filtered, if necessary) before reaching the recipient(s). In addition, the mail servers are configured to prevent inappropriate internal or external email relay. One can assume Exchange 2000 is securely integrated into GE's Windows 2000 network infrastructure.

Name Resolution

The external DNS servers respond to name resolution queries for the company's Internet registered domain names as well as for the GreatProducts web site. These servers also resolve Internet domain names for internal users. The external DNS servers use the Windows 2000 DNS server. The zone records on this server are for Internet domains only – zone information for the DMZ domain (ge.dmz), or the internal domain (ge.corp), is not stored on these servers.

The internal DNS servers are configured to forward all queries that cannot be resolved by internal DNS servers to the external DNS servers. Additional details of the company's DNS structure are discussed later. DNS services for the DMZ domain are integrated into Active Directory.

DNS is a critical component of any network infrastructure. One can assume GE's DNS infrastructure is secure, redundant, and provides for an acceptable level of performance. The company's network teams regularly monitor DNS services.

Remote Access

The Windows 2000 Routing and Remote Access (RRAS) servers in the DMZ exist for two purposes. First, connectivity between the Hampton office and the BCC is achieved

through an Internet VPN. Second, traveling employees and executives require remote access to the GE network.

RRAS1 is the Hampton side of a dedicated VPN tunnel to the BCC. RRAS2 is the BCC side of the VPN tunnel. GE has configured a router-to-router VPN tunnel secured by IPSec operating in transport mode. This allows all communications between the Hampton office and the BCC to be securely transmitted across the Internet, allowing GE to realize cost savings by not purchasing a dedicated leased line between the two sites. The two servers supporting this VPN are robust and have IPSec offload cards to improve performance. One can assume the VPN is securely configured with appropriate packet filtering, secure key exchanges, appropriate re-keying intervals, and encryption levels adequately set.

RRAS3 is the VPN server for remote clients. This server allows remote users to securely connect to the GE network to synchronize Outlook, submit time and expenses through the company's time reporting system, as well as access network file shares. This server also has a bank of modem interfaces, which allow users to dial-in to the GE network if Internet access is not available.

RRAS1 and RRAS3 have a second interface connected to GE's internal network. GE has chosen to route traffic directly to the internal network rather than through the firewall for performance reasons. Connection profiles are used to provide additional security for remote access connections. This situation is the one exception to GE's policy that requires all inbound and outbound traffic to route through the firewall.

Web Servers

Several web servers running Internet Information Services (IIS) are in the DMZ. GE's company web site serves static content providing information about the company and its products and services. The web servers hosting the GreatProducts site for LED Corp. are also in the DMZ. Multiple servers host each web site for redundancy and performance purposes.

DNS round robin is the method used to load balance incoming traffic to the GreatProducts web site. The firewall is configured with specific rules permitting communication between the IIS servers supporting LED's GreatProducts site and the backend SQL Server databases. Currently, a dedicated service account with restrictive permissions is used authenticate to the databases. A customer identifier is used to separately log the transactions performed by customers. In the future, GE expects to incorporate functionality allowing user accounts to be impersonated so that authentication and authorization can be controlled at a per user level within the application.

Internal Network

The majority of GE's servers, workstations, and databases are located in the internal network segments. The company uses the private network address range 10.x.y.z and internal subnets are appropriately sized to accommodate anticipated growth and optimize performance. The firewall permits no connections from the Internet to be made to hosts in this segment. Several hosts in the DMZ are permitted to connect to hosts in the internal network, such as when web servers supporting the GreatProducts site require access to backend databases.

The internal network has three main segments – the EasyOrder Segment, User Segments, and a Services Segment. The network is structured this way to increase performance and improve security. Each segment and the hosts located in the segment are discussed below.

EasyOrder Segment

The EasyOrder Segment contains the hosts that support the company's outsourcing arrangement with LED Corp. The backend databases supporting the EasyOrder application reside here. These databases store application variables, customer data, and transaction records, as well as other information for the GreatProducts web site. In addition to the databases, several IIS web servers also reside here. These servers permit call representatives in the BCC to place orders for customers ordering over the telephone. In addition, the operational employees that monitor and support billing and order fulfillment notices also access application functions through IIS.

Due to the sensitivity of the data in the segment, network access controls regulate the hosts and protocols permitted to access the EasyOrder servers. This segment will support additional web servers and databases for other companies that may outsource order and billing operations to GE. As additional customers outsource these functions, the company will have to consider how it will manage multiple sets of customer data with differing storage, privacy, access control, and recoverability requirements.

User Segments

All user workstations (including laptops) at the Hampton office run the Windows 2000 Professional operating system. GE has retired all Windows 95/98/NT workstations and the older hardware used to support them. This allows the company to effectively and efficiently control security parameters and patch levels across the user population. The company has implemented desktop security through Group Policy.

DHCP is used to configure the user workstations with several network attributes including IP address, default gateway, primary and secondary DNS servers, and primary DNS suffix. All servers and databases in the GE network are configured with static IP addresses. GE has configured super scopes on several servers using the 80/20 rule. In this configuration, a "primary" DHCP server can allocate 80 percent of the addresses in a scope and another server can allocate the remaining 20 percent of the available IP addresses. This helps improve the fault tolerance of this important network

service. The servers supporting DHCP also support network printing functions. DHCP and printing are consolidated due to the relatively low load each service places on the host. Servers supporting DHCP and printing are positioned on subnets local to users, thus helping to improve performance.

A domain controller for the ge.corp domain, DC2, is also positioned on a user segment local to the majority of GE's user population. This server processes the majority of computer and user logons and directory queries. Domain controllers are also DNS servers in GE's network environment. The design and security of this domain are discussed later in additional detail.

Services Segment

The hosts connected to the Services Segment provide core network services to the company. This segment is essentially the backbone of the network and exists to segregate certain servers away from the majority of users. Access controls exist to permit only certain types of traffic to flow in and out of the segment. The key hosts located in the Services Segment are described below.

- *Internal Mail:* This Exchange 2000 server supports email distribution and delivery. Like the external mail server, antivirus and content filtering controls are in place to help protect against email related threats. The internal mail server forwards email addressed to external recipients to the external mail server. The external mail server relays emails from the Internet to the internal mail server. This server, like the external mail server, is configured to prevent inappropriate email relay.

- *Domain Controller (DC1):* The root domain controller for the ge.corp domain resides on this segment. As discussed later, this DC is the owner of all operations master roles. The domain controller is located on this segment to help improve the overall performance of AD while protecting the critical functions this DC provides.

- *IIS Web Servers:* An intranet exists to support GE users. Through the intranet, employees can obtain contact information for other employees as well as access policies and procedures.

- *RRAS Connectivity:* The VPN routers in the DMZ, RRAS1 and RRAS3, connect directly to this segment. This allows remote users efficient access to applications and files.

- *File Servers:* GE currently shares files by publishing shares in Active Directory and securing the shares with NTFS permissions assigned to local security groups. All shares are published under the Files OU (discussed later). The company is currently planning an AD integrated Distributed File System (DFS) infrastructure.

- *Other GE Servers:* GE has several other hosts supporting the company's business applications. Separate applications and databases residing in this segment support

company functions such as time and expense reporting, payroll/accounting, as well as customer relationship management. When implemented, the certificate services infrastructure will reside in the Services Segment too.

Blacksburg Call Center Segment

The Blacksburg Call Center (BCC) location is in a different geographic location than the company's other network segments. Connectivity between the BCC and the Hampton office is achieved through a dedicated VPN connection. RRAS2 is the endpoint of the VPN tunnel on the BCC side. Connectivity to the Hampton office through the VPN is the only type of connectivity permitted; direct access to the Internet through the BCC's Internet connection is not permitted. As the BCC grows, management recognizes it may be necessary to invest in a dedicated connection between the two sites. The network functions supported by other hosts in the BCC such as the domain controllers and DHCP/Print servers are the same as those previously discussed.

Active Directory Design: ge.dmz

An AD domain exists in the DMZ. This domain is named ge.dmz. The domain exists solely for administrative purposes and is not used to manage any internal or external users. Only administrators have accounts in the domain. This domain allows the company to realize the following benefits.

- Consistent and secure configurations are in place on all servers by leveraging Group Policy.

- Security patches and other software updates such as service packs can be expeditiously deployed to help ensure security vulnerabilities are promptly corrected.

- Administrative accounts are maintained through the directory rather than being managed individually on separate servers. A strong password policy is enforced, requiring passwords to be long and complex and changed on frequent intervals. Most local accounts are disabled. Those local accounts that are not disabled are assigned long pass phrases. Because these accounts are rarely used, audit logon events related to these accounts are investigated.

- A separate domain in the DMZ with no trust relationships between the internal (ge.corp) and external (ge.dmz) domains provides two security benefits. First, the separate domain presents numerous barriers for internal users attempting to probe and access the hosts supporting the company's Internet presence. For example, user workstations are not joined to the ge.dmz domain; therefore, common users would have to discover a workstation joined to the domain before they could even attempt to access any DMZ resources by logging on to through the domain. Second, if the domain in the DMZ is compromised, the attacker would only be able

to access a limited number of company resources. Servers storing information such as the EasyOrder source code, product pricing, and marketing strategies are all located in the internal domain. Accounts in the DMZ domain are different from those in the internal domain, so compromising DMZ accounts will not lead to compromising internal accounts.

The focus of this description of GE's network and AD environment is on the internal network. Therefore, the specific security policies and controls used to secure externally accessible hosts are not discussed here. GE anticipates the number of hosts in the DMZ to steadily grow over the next several quarters and has implemented this domain to ensure all production servers can be controlled in a secure, consistent manner. One can assume strict security policies are implemented on all hosts in the DMZ. IPSec packet authentication, packet filtering, and host based intrusion detection software are just some of the other security controls implemented in the DMZ.

Active Directory Design: ge.corp

The IT infrastructure is centrally managed from the Hampton site. Administrators in Hampton are responsible for ensuring the network is stable and available to support the business. Monitoring, capacity planning, network/application troubleshooting, and change management are just some of the processes performed in Hampton. A small IT support staff at the BCC helps manage and administer computing needs at that location. Administrative capabilities are delegated to this support staff to allow better support for BCC computing needs while retaining centralized control and maintaining security.

GE has implemented a single Active Directory domain to support the company. This domain is named "ge.corp." Prior to the deployment of Windows 2000, GE maintained several different domains, including a separate domain for the call center in Blacksburg. During the transition to Windows 2000, the company redesigned the logical structure of the network. Management implemented a single domain AD architecture for several reasons.

- The single domain design fits well with GE's IT management structure. The majority of IT management is performed in Hampton and the limited amount of administration performed in Blacksburg is securely delegated. Management does not have any reservations about allowing certain trusted administrators to have full control over all objects in the domain, including those in the BCC.

- Because the company only supports one domain, the hardware assets previously used to support multiple Windows NT domains are either retired (saving server licensing costs) or now provide a greater level of fault tolerance. A complete replica of the full AD database is stored on four separate servers across two physical locations.

- AD easily scales to accommodate GE's approximately 500 employees and other directory objects (e.g., computers, group policies, etc.). One domain is more than sufficient to support the company's current growth plans.

- The connectivity between the Hampton site and the Blacksburg site is more than adequate to support directory replication. Creating a separate domain solely to avoid replicating across a WAN could not be justified.

- Access control schemes are easier to implement, thus increasing security while easing administrative burden. Administrators no longer manage trust relationships and all access controls are assigned to local groups in the domain (although in some cases, permissions may assigned individually if necessary).

Note: A second GE domain exists in the DMZ. This domain is for administrative purposes only. The domain does not hold any user accounts, replicate outside of the DMZ, or extend in any way outside of its network segment.

Several published authorities also favor the single domain design implemented by GE. In addition to the SANS Institute (Fossen, 5.1, p.156), Microsoft states, "a structure consisting of one domain that is simultaneously one forest consisting of one tree is not only possible, but may be the optimal way to organize your network" (Microsoft Corporation, "Active Directory Architecture"). The authors of *Windows 2000 Server Architecture and Planning* (Nielson, p.210) as well as *Inside Windows 2000 Server* (Boswell, p.467) also indicate that a simple, single domain design is preferred.

The ge.corp domain is in native mode and thus does not replicate with any legacy domain controllers. All client workstations run the Windows 2000 Professional or Server operating system. The following sections focus on three important aspects of the AD infrastructure – Domain Name System (DNS), special purpose servers such as those that host the Global Catalog, as well as how objects are grouped, managed, and assigned access rights with organizational units (OU) and groups.

Domain Name Service (DNS)

DNS is a critical element of Active Directory design. Hosts query DNS for a variety of important operations such as identifying DCs during network logon. GE has implemented a private DNS domain (ge.corp) on the internal network. This name was chosen because it does not exist on the Internet, and clearly differentiates the company's internal and external (giacenterprises.com) DNS namespaces. GE has a one-to-one mapping between the DNS domain name and the AD domain name (i.e., both are ge.corp).

Each GE site has two DNS servers. The company's DCs also serve as DNS servers that host an AD integrated zone for the domain. When DNS is integrated into AD, zone records become part of the AD database and are included in directory replication. GE's

internal namespace design and DNS implementation provide the following benefits to the company.

- Positioning DNS servers in each site reduces network traffic and improves query response time because a local server processes most DNS queries.

- The fault tolerance of DNS and AD is improved by integrating zones into the directory. Each location has two DNS servers, reducing the likelihood a DNS failure could impact the availability of AD.

- DNS management is simplified because GE does not manage and maintain a DNS infrastructure (e.g., primary and secondary DNS servers, replication topology, etc.). In addition, administration is simplified because no overlap exists between internal and external zones. Each zone is separate and is independently managed (Nielson, p. 200).

- Using a different namespace internally and externally simplifies name resolution for internal clients as well as administration. GE does not duplicate any external DNS records on internal name servers (Microsoft Corporation, "Planning Your Namespace").

- The short DNS suffix used internally by the company is friendly to the user community.

The company's network teams regularly monitor DNS performance. One can assume the DNS infrastructure is implemented in a secure manner. For example, in addition to the database redundancy benefits provided through Active Directory, the company has configured each DNS server to require secure updates, helping to protect the integrity of DNS records.

Operations Masters and Global Catalog Servers

Servers that provide Flexible Single Master of Operations (FSMO) roles and/or host the Global Catalog (GC) are critical for helping to ensure the integrity and stability of the AD database. In some situations, such as in multi-domain environments or as a result of performance considerations, it is necessary to distribute FSMO roles across multiple servers. Several sources, including Microsoft ("Active Directory Architecture") and the SANS Institute (Fossen, 5.1, p.104), recommend placing at least one GC per site and, in multi-domain environments, avoid assigning the Infrastructure Master role to a GC server.

GE's management of FSMO role masters and GC servers is simplified and provides a sound foundation for AD.

- The first DC in the domain, DC1, is the owner of all FSMO roles. This DC is connected to the backbone of the network to help ensure optimal network connectivity to other DC's and GE hosts. Network administrators diligently monitor performance and event logs on DC1 (as well as all other critical network hosts). Contingency plans exist that describe how the company will transition FSMO roles in the event DC1 becomes permanently unavailable.

- All domain controllers in both sites host a GC. Each DC is already hosting a full replica of the AD database and configuring each server with a global catalog helps improve the performance of user logons and directory queries.

- Placing two DC/GC servers in each site provides redundancy. The loss of a DC in either site will not prevent users from accessing the network, although performance may be slightly impaired. The loss of two domain controllers in one site would affect performance; however, users could still gain access to network functions (file access, printing, etc.) until a DC local to their site is brought back online.

Sites and Replication

GE has implemented two sites, HPT and BCC. These sites reflect the two physical locations from which the company operates: Hampton and Blacksburg. The company does not manage intra-site replication. Replication occurs as needed (i.e., every five minutes or when a change to the directory occurs) and the Windows 2000 Knowledge Consistency Checker (KCC) manages intra-site replication topologies at the Hampton office and the BCC. The replication schedule for the "HPT to BCC" site link has been adjusted so that inter-site replication occurs every 45 minutes. GE's network management team has determined this replication interval does not hinder the performance of the VPN connection.

Separating the ge.corp domain into two sites localizes replication traffic and improves the performance of the VPN connecting the Hampton office to the BCC. Replication traffic occurs only on scheduled intervals (in this case, every 45 minutes) rather than as updates are made to the directory. An additional benefit of implementing sites is to help localize client queries. For example, when a client queries DNS to identify a DC for network logon, it includes the last site name stored in its registry. DNS returns the service (SRV) DNS records identifying domain controllers in the client's site. The client pings each domain controller returned in the query and the DC compares the client's subnet to the subnet objects configured in the directory (by the AD Sites and Services console). If the client's IP subnet does not match the subnet of the DC's site, the DC refers the client to a different, local domain controller in its site (Boswell, p.648).

One drawback to implementing sites is the delay introduced into directory replication. By default, inter-site replication occurs every 180 minutes. The 45 minute directory replication delay introduced by GE's configuration is acceptable to management, especially considering the reduction in VPN traffic. The replication delay is acceptable

because significant changes to the directory do not occur frequently. Administrators use the "Update Now" option whenever important changes, such as changes to security settings in Group Policy, are made that require immediate replication throughout the directory.

Organizational Units

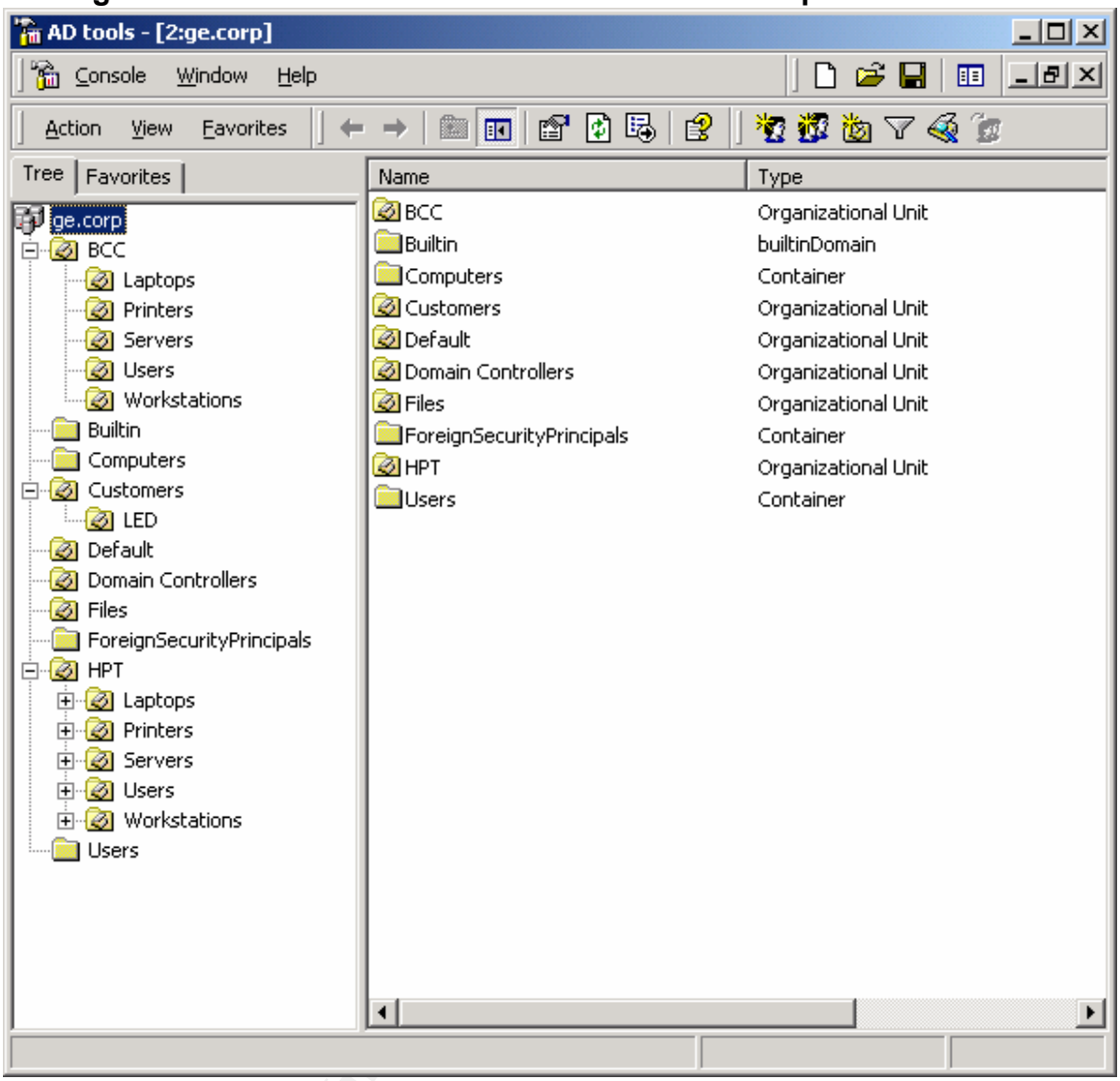
Overview

An organizational unit is the primary container used for organizing objects and applying policies in Active Directory. OU's also provide the mechanism for delegating authority within the directory. The OU hierarchy implemented at GE sought to achieve these goals:

- Provide a directory structure that is logical and easy to understand and navigate;
- Flexibly accommodate the addition of new locations and/or customers; and
- Facilitate securely delegating authorities within the directory.

GE designed its OU structure around the company's different locations and its customers. For example, each site (e.g., HPT and BCC) has its own OU. Within each site OU, child OU's exist for laptops, printers, servers, users, and workstations. A screen display from the Active Directory Users and Computers MMC console is displayed below. A logical diagram of the Directory is presented in Appendix B.

GE Organizational Unit Structure – AD Users and Computers Console



OU Functional Overview

The table below describes the certain organizational units (or in some cases, containers) in the domain.

OU	Purpose
Site OU's	
Sitename (ou= *Sitename*,dc=ge,dc=corp)	▪ The *Sitename* is the name of a specific site in the company (e.g., HPT or BCC) ▪ One site OU exists for each physical location ▪ Container for other, more specific site OU's
Computers (ou=*Computers*,ou= *Sitename*,dc=ge,dc=corp)	▪ *Computers* can be Laptops, Servers, or Workstations ▪ Container for computer objects ▪ Permits custom policies and delegation of authority based on the type and role of the computer object
Users (ou=Users,ou= *Sitename*,dc=ge,dc=corp)	▪ Container for User objects ▪ Permits custom policies and delegation of authority based on the type and role of the user object ▪ Contains security global groups used to organize users for access control
Printers (ou=Printers,ou= *Sitename*,dc=ge,dc=corp)	▪ Container for Printer objects local to the site
Customer OU's	
Customers (ou=Customers,dc=ge, dc=corp)	▪ Container object of the OU's for each GE customer ▪ Currently holds one OU – LED ▪ Additional child OU's will be created as the company's client base expands
LED (ou=LED,ou=Customers, dc=ge,dc=corp)	▪ Container object for the LED Corporation ▪ Currently holds the internal web servers and databases for the GreatProducts site ▪ This OU will hold security local groups required by future versions of EasyOrder for user authorization
Other OU's	
Files (ou=Files,dc=ge,dc=corp)	▪ Files shares published in AD ▪ Positioned at the top of the OU hierarchy to improve the performance of user queries

OU	Purpose
Domain Controllers (ou=Domain Controllers,dc=ge,dc=corp)	▪ Default domain controllers organizational unit ▪ Holds domain controllers for the ge.corp domain ▪ The Default Domain Controllers Policy, customized to meet GE's needs, is applied on this object
Default (ou=Default,dc=ge,dc=corp)	▪ Container for user and group objects created in the Users container during installation ▪ Contains sensitive accounts and groups (e.g., the Schema Admins group)
Users (cn=Users,dc=ge,dc=corp)	▪ Not used – All objects in this container have been moved to the Default OU
Builtin (cn=Builtin,dc=ge,dc=corp)	▪ Container for the Builtin groups (e.g., Account Operators, Backup Operators, etc.) ▪ With the exception of the Administrators group, GE does not generally use Builtin groups ▪ The Builtin groups do not have any accounts associated with them – particularly the "Pre-Windows 2000 Compatible Access" group ▪ Groups such as Domain Admins, DnsAdmins, Schema Admins are installed in the Users container by default and have been moved to the Default OU

OU Design Benefits

Some of the benefits of this Active Directory design that were considered by management are described below.

- The OU hierarchy is simple and allows objects to be easily located and organized within the directory. By organizing objects by site, users and administrators can easily locate objects. For example, in this structure users can quickly browse the directory and locate all printers at their location. Directory permissions can be easily to configured to restrict viewing privileges to only those necessary groups.

- The IT support group at the BCC can be delegated the privileges to add and remove user, workstation, and laptop accounts only at their site. As this center grows and the support group assumes additional responsibilities, the directory design allows additional authorities to be gradually delegated as appropriate. Additional physical locations can be easily added to the directory without upsetting directory design. As the responsibilities of support staff at these new locations increase, authority can be delegated to these groups as well.

- Currently, GE has only one client, LED Corp., which has outsourced operations to the company. However, the company's strategic plan is to acquire additional customers through the outsourcing channel. Certain benefits of the directory design were attractive to management with respect to the addition of new clients. Additional clients will not upset the directory design. A separate OU for each company allows for custom security policies to be assigned for each company's web servers and databases. As the number of clients grows, dedicated administrators could be assigned to each OU. Also, a new client may wish to use their existing customer support staff but still have GE host the EasyOrder application and database. The separate OU's facilitate future trust relationships that may be required or delegating authorities to other administrators.

- Future versions of the EasyOrder application currently in the quality assurance phase begin to leverage AD for authentication and authorization. With this requirement, an appropriate group (e.g., a group of managers responsible for a specific client) could be delegated the authority to add, move, and remove user accounts to/from security global groups related to each customer. These security global groups are placed in security local groups used by the application for authorization. As new call centers are added to the directory, new global groups could be created and separately managed on a per client basis in each OU, easily allowing multiple centers to service the same clients. Administrators will control the membership of local security groups for each client.

- The Files OU located high in the directory tree improves the performance of directory queries for file shares. Because individuals from multiple locations may potentially access these file shares, creating a separate OU for these objects is more logical than placing them in a particular site's container.

Important Groups and Delegation of Authority

Security global groups (global groups) and security local groups (local groups) are used throughout the domain to organize users, assign permissions to resources, and delegate authorities. In general, users are grouped in global groups for organizational purposes. Permissions to common resources on file shares are assigned to local groups. By placing global groups into local groups, permissions are indirectly assigned to users.

Two primary categories of groups exist in the domain. Administrative Groups have special permissions on servers and OU's. Business Groups exist to reflect access control requirements of different business units.

Administrative Groups

Administrative Groups exist to restrict and segregate powerful authorities in the directory as well as on domain controllers, member servers, and workstations. The key administrative groups in the ge.corp domain are Domain Admins, Workstation Admins,

Server Admins, and BCC Admins. The membership of these groups is enforced through Group Policy. A summary of each group, and the authorities delegated to the group are listed in the table below.

Group	Description
Domain Admins	▪ Have full control on all directory objects ▪ Power is virtually unlimited ▪ Membership is restricted to two (2) trusted administrators
Workstation Admins	▪ Group includes members of GE's Help Desk/Desktop Support team in the Hampton office ▪ Delegated the authority to change passwords in the Users OU ▪ Permitted to add workstations to Laptops and Workstations OU's only ▪ Have local administrative privileges on laptops and workstations ▪ Cannot modify GPO's associated with the Laptops and Workstations OU's
Server Admins	▪ Group includes the administrators in GE's Hampton office ▪ Permitted to logon locally to all domain controllers and member services ▪ Restricted from performing operations in Laptops or Workstations OU's ▪ Can perform most domain/server administrative functions in the directory except for those such as modifying the schema or creating domain level objects such as OU's
BCC Admins	▪ Group includes the on-site support staff for the Blacksburg Call Center ▪ Group is empowered to administer and troubleshoot file, print, and DHCP functions ▪ Permitted to add users and workstations to the BCC OU's only; permitted to change passwords, unlock accounts, etc. ▪ Local administrators on all workstations in the OU for troubleshooting purposes ▪ Cannot administer domain controllers ▪ Cannot create/modify GPO's

Business Groups

Each GE unit has one or more groups associated with it. For example, two groups exist for Human Resources: HR and HR Managers. These groups were created because of different access control requirements to various types of information. For example, only

HR Managers are permitted to access personnel information related to corporate executives. Separate groups exist for Finance, Development, Quality Assurance, Executives, Sales, and Operations.

A primary reason for the group infrastructure is assigning access rights to various shares on network file servers. Another important use for groups is restricting application access. Some applications used by the company either require users to belong to certain application groups or have read/write access to application configuration files or databases. The Human Resources application is one such application. Users must belong to the Human Resources security global group to logon to the HR application. The HR security global group has been assigned read access to several INI files that are required to launch the HR application client. This provides additional level of control to the application. Not only to users have to be configured within the application and have an application client installed on their workstation, they must also be assigned the Human Resources group.

Group Policy and Security

Group Policies provide an effective and efficient method for performing a variety of administrative tasks such as ensuring appropriate security configurations are enabled on servers and workstations. When developing GPO's for use in the ge.corp domain, GE used templates from the NSA to establish a security baseline, and then modified that baseline using recommendations from the SANS Institute as well as the Center for Internet Security. Finally, administrators considered the unique needs of GE's network environment as well as corporate security policies.

In general GE's GPO's apply to either Computer Configuration or User Configuration, but not both. This is done for simplicity. When possible, the "Disable Computer Configuration settings" or "Disable User Configuration settings" has been selected on the GPO. Disabling non-applicable sections of GPO's "expedites startup and logon for those users and computers subject to the Group Policy object" (Microsoft Corporation, "Group Policy→ Best Practices").

Note: Hundreds of parameters can be configured through Group Policy. In addition, custom templates can be developed to configure any registry value. Thus, it is not practical or feasible to discuss every possible option here. Important Group Policy options are discussed in this section. One can assume those options not discussed are securely configured to values consistent with recommendations published by the National Security Agency, Center for Internet Security, SANS Institute, and/or Microsoft.

Domain Group Policy

The Domain Group Policy object (GPO), "Default Domain Policy," contains high-level settings that are pervasive across the domain. The settings configured at this level are

acceptable for all network hosts and/or users. Some of the parameters configured by this policy can only be configured at the domain level (e.g., password parameters). The "No Override" option is enabled on this policy further ensuring no other GPOs modify the domain settings.

GE used the domain policy developed by the NSA (W2k Domain POLICY.INF) as the baseline security configuration for the domain. This security template significantly increases the strength of password and account lockout parameters. The default Windows 2000 domain policy does not require strong passwords or enforce reasonable password parameters (e.g., blank passwords are permitted). Passwords not only help secure user logon, but also serve other purposes such as helping to secure a user's private keys.

The following areas were considered when creating and tuning the domain GPO.

- The implementation of strong password requirements created high call volumes to the help desk. Rather than decreasing the "Minimum password length" parameter, GE disabled the "Password must meet complexity requirements" parameter. This change alleviated excessive calls to the help desk after users were trained to use easy-to-remember pass phrases.

- The "Account lockout threshold" was increased from three invalid logon attempts to five invalid logon attempts. This setting is more forgiving for end users while still protecting against brute force attacks. The resulting password and account lockout parameters for the ge.corp domain policy are summarized in the table below.

Parameter	Value in the ge.corp Default Domain Policy GPO
Password Policy	
Enforce password history	24 passwords remembered
Maximum password age	90 days
Minimum password age	1 days
Minimum password length	12 characters
Passwords must meet complexity requirements	Disabled
Store password using reversible encryption for all users in the domain	Disabled
Account Lockout Policy	
Account lockout duration	15 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	15 minutes

- After evaluating performance during a trial period, GE decided to continue using the more secure Kerberos parameters recommended by the SANS Institute (Fossen, 5.1, p.59). Specifically, the "Maximum Lifetime for a Service Ticket," has been set to 60 minutes, and the "Maximum Lifetime for a User Ticket" has been set to one (1) hour. These parameters help protect against the risk an intruder may use old Kerberos tickets to gain access to systems or data.

- GE has implemented a warning banner at the domain level. GE used the verbiage from the Defense Department's warning banner as a baseline, and ensured the company's legal team approved the wording prior to implementation. This banner is implemented in the "Message text (title) for users attempting to log on" security option.

- Restricted Groups – Restricted Groups are configured at the domain level. Group Policy is used to explicitly define the membership in security sensitive groups as well as define which groups security sensitive groups can be "members of." The key groups configured by the part of the policy are the Domain Admins, Schema Admins, Everyone, Workstation Admins, Server Admins, and BCC Admins groups.

Domain Controller Group Policy

The Default Domain Controllers Policy object contains security settings for the company's domain controllers. This GPO is linked to the default Domain Controller OU. The baseline for this GPO is the NSA's domain controller security template (W2kDC.INF). GE has made some modifications to this baseline to better fit the company's environment. Some important security enhancements improving security above the default levels are listed below.

Security Element	Enhancement/Description
Access Control User Rights: "Access this computer from the network" and "Log on locally"	▪ Permissions for accessing the domain controller from the network as well as console logon are restricted. ▪ Administrators, Authenticated Users, and Enterprise Domain Controllers are permitted to access the computer from the network. ▪ Only members of the Administrators group are permitted to logon locally.

Security Element	Enhancement/Description
Authentication Protocol Security Options: "LAN Manager Authentication Level"	▪ GE has thoroughly inventoried all application and operating system software. GE has verified the LM and NTLMv1 protocols are not in use. Therefore, the "LAN Manager Authentication Level" security option is configured to send NTLMv2 responses only and refuse the LM and NTLMv1 protocols. ▪ The LM and NTLMv1 protocols are supported by Windows 2000 for backwards compatibility. These authentication protocols are not secure.
File System Access Computer Configuration/ File System	▪ Default NTFS permissions are not adequate. The NSA template makes numerous enhancements, only some of which are described here. ▪ Permissions for the root drives of all partitions are set to Administrators and SYSTEM: Full Control, Authenticated Users: Read and Execute, List Folder Contents, and Read. ▪ Permissions on the Program Files folder, SystemRoot (i.e., \winnt) folder, and the SystemDirectory (i.e., \winnt\system32) are more secure. Administrators and SYSTEM: Full Control, Authenticated Users: Read and Execute, List Folder Contents, and Read. ▪ Template permissions for the NTDS and SYSVOL folders have been changed to reflect their actual drive locations. ▪ On some important files and folders, auditing has been enabled. The specific files and folders configured for auditing are not discussed here.
Available Services Computer Configuration/ System Services	▪ GE disables all services that are not used. ▪ Several services enabled by default are disabled in GE's environment. These include the Alerter, ClipBook, Computer Browser, Fax Service, Messenger, NetMeeting Remote Desktop Sharing, and Telnet services. ▪ The permissions on all services are set to allow only Administrators and SYSTEM to start, stop, or pause a service.
Registry Access Computer Configuration/ Registry	▪ The security template used has numerous registry permissions defined. GE has not altered the default template permissions. ▪ The registry permissions defined help secure most important keys such as HKLM\software and HKLM\system. ▪ The permissions assigned to most keys allow Full Control to the "root" level key to Administrators and SYSTEM, while those groups and CREATOR OWNER have Full Control on

Security Element	Enhancement/Description
	Subkeys. ▪ Registry permissions allow Authenticated Users Read and Execute permissions in most cases.
Physical Media Security Options: "Allowed to eject removable NTFS media" "Restrict CD-ROM access to locally logged on user only" "Restrict floppy access to locally logged on user only"	▪ The security options related to removal media have been configured to further augment physical security controls. This is especially important at the BCC, where physical security controls are only somewhat secure because access cannot be restricted solely to GE's trusted administrators in the Hampton office. ▪ Removable NTFS media such as ZIP drives are not used on any domain controllers. This option is assigned only to Administrators. ▪ GE permits only users (Administrators) accessing the computer at the local console to access the CD-ROM and floppy disk drives.
Auditing and Event Log Computer Configuration/ Local Policies/ Audit Policy Computer Configuration/ Event Log Security Options: "Audit use of Backup and Restore Privileges" and "Shut down system immediately if unable to log security audit"	<u>Auditing</u> ▪ The security template used makes significant improvements to default auditing and event log settings. By default, Windows does not audit any events. ▪ The Audit Policy settings for the domain controllers are: ➢ Audit account logon events: Success, Failure ➢ Audit account management: Success, Failure ➢ Audit directory service access: Failure ➢ Audit logon events: Success, Failure ➢ Audit object access: Failure ➢ Audit policy change: Success, Failure ➢ Audit privilege use: Failure ➢ Audit process tracking: Not defined ➢ Audit system events: Success, Failure ▪ The Audit Policy in place allows GE to collect a sufficient amount of security and operational audit and event records. ▪ Process tracking is not audited, and only failures and logged for object access and privilege use due to system performance considerations. ▪ The "Audit use of Backup and Restore Privileges" security option enables auditing of <u>any</u> use of a user right. GE has enabled this policy. ▪ The "Shut down system immediately if unable to log security audits" security option is disabled. Management feels monitoring efforts are sufficient and does not want to risk a system shut down for this reason. ▪ In addition to the auditing settings discussed here, GE also

Security Element	Enhancement/Description
	audits access to some important files and folders. The specific files and folders audited by GE are not discussed here. ▪ In addition to the auditing settings discussed here, GE also audits actions on some important AD objects. The specific Active Directory object and containers audited by GE are not discussed here. <u>Event Log</u> ▪ GE sized the physical disks on each domain controller to permit application, security, and system logs of approximately 4 GB. The Event Log settings are configured to reflect this size. ▪ GE overwrites the event logs after records are seven days or older. GE performs full backups of event logs on a daily basis. ▪ The "Shut down the computer when the security audit log is full" is disabled. Management feels monitoring efforts are sufficient and does not want to risk a system shut down for this reason.
Installation Behavior Security Options: "Unsigned driver installation" and "Unsigned non-driver installation"	▪ GE has configured the unsigned driver and non-drive installation options to "Do not allow installation." ▪ In the event unsigned updates are required to device and non-device driver software, this setting is temporarily changed after the update has been evaluated in the test environment and approved by the change management process. In general, the Windows Hardware Quality Lab (WHQL) certifies most updates of this nature. ▪ This helps prevent the accidental installation of driver software that has not been certified by Microsoft and could lead to system malfunction.

Security Element	Enhancement/Description
System Shutdown User Rights: "Force shutdown from a remote system" and "Shut down the system" Security Options: "Allow system to be shut down without having to log on"	▪ The System Shutdown options are restricted only to Administrators. ▪ All remote restarts of domain controllers are performed with the shutdown.exe utility.
Anonymous Access Security Options: "Additional restrictions for anonymous access"	▪ This security option has been set to, "No access without explicit anonymous permissions." This security option is used to help reduce security exposures posed by null sessions and unauthenticated users.
Secure Channel Protection Security Options: "Secure channel: Digitally encrypt or sign secure channel data (always)" "Secure channel: Digitally encrypt secure channel data (when possible)" "Secure channel: Digitally sign secure channel data (when possible)" "Secure channel: Require strong (Windows 2000 or later) session key"	▪ The Secure Channel is the RPC NetLogon channel that protects user and computer logon as well as other functions such as password changes. ▪ All secure channel options are enabled, including the strong session key option. All clients are Windows 2000 Professional and configured with the same secure channel settings through Group Policy.
Renamed Accounts Security Options: "Rename administrator account" and "Rename guest account"	▪ GE does not rename user accounts. ▪ The Administrator account has a complex and lengthy pass phrase and is not generally used.

General User Policy

A wide range of User Configuration options are available through Group Policy to help secure the environment and control the user's experience. GE does not make use of these configuration options available to the fullest extent. GE tries to foster a positive

work environment and management decided significant controls on user workstations would create negative attitudes towards management and the company.

The General User Policy provides a baseline configuration providing general security settings that are pervasive across all users. This GPO implements some levels of security while still allowing the user to access most workstation functions. Some of the important elements of the General User Policy are described below.

Security Element	Enhancement/Description
Internet Explorer User Configuration/ Windows Settings/ Internet Explorer Maintenance User Configuration/ Administrative Templates/ Windows Components/ Internet Explorer	▪ Using the Internet Explorer browser is required by company security policy. The IT staff works to ensure IE levels are securely and consistently deployed. ▪ Connection settings are configured for Internet access. ▪ URL's to commonly used locations on the company web site are configured for the users' Favorites menu. Company sites are located in the "Local intranet" zone that permits a higher level of trust for web scripts and executables. ▪ Users are prevented from accessing IE menus such as "Security," "Content," and "Connections." ▪ File size limits are in place so that cached pages are periodically purged. ▪ Appropriate levels of security are implemented in the Internet zone to help reduce the affects of harmful scripts and applets.
Screensaver Protection User Configuration/ Administrative Templates/ Control Panel/ Display "Hide Screen Saver tab" "Activate screen saver" "Screen saver executable name" "Password protect the screen saver" "Screen Saver timeout"	▪ GE uses screen savers are used as a control to help prevent station hopping. ▪ Screen saver password protection is enabled and timeouts are set at 1920 seconds. ▪ A custom company screen saver is used that puts a minimal load on the processor and graphic display adapter. ▪ The "Hide Screen Saver tab" policy prevents users from using the Control Panel to add, configure, or change screen saver settings.
Restricted MMC Consoles	▪ GE proactively restricts the MMC consoles average users are permitted to access. For example, typical users are not

Security Element	Enhancement/Description
User Configuration/ Administrative Templates/ Windows Components/ Microsoft Management Console/ Restricted/Permitted snap-ins	permitted to access AD snap-ins such as Active Directory Sites and Services. Although other controls also restrict this activity, restricting MMC consoles provides an additional layer of security. ▪ The specific MMC console restrictions implemented for users are not discussed here.
Folder Redirection User Configuration/ WindowsSettings/ Folder Redirection	▪ Important user folders such as "My Documents" are redirected to file shares. This helps to ensure user data is included in nightly backups. ▪ This section of the policy is modified depending on which OU the GPO applies. The Advanced option is used to specify locations for various users based on their security group. This helps ensure files are redirected to local file servers.
GPO Processing Computer Configuration/ Administrative Templates/ System/ Group Policy "Apply Group Policy for computers asynchronously during startup" "Apply Group Policy for users asynchronously during logon"	▪ Asynchronous GPO processing permits users to access their desktops before GPO processing is complete. By default, this behavior is disabled. GE has left the default behavior in place. ▪ GE encourages all users to allow their machines to complete startup, complete disk checks, etc. prior to logging on or performing other functions, such as connecting PDA's.

Workstation Security Policy

One aspect of network security that GE did not overlook is the importance of implementing security controls at the desktop level. By standardizing on the Windows 2000 Professional desktop operating system, the company can implement additional security controls to the level where a variety of threats originate. Two considerations evaluated prior to implementing workstations security are noted below.

- Internal users could compromise workstations and load tools such as keystroke loggers to obtain the password of an individual who has access greater than their own. The attacker could then use that user name and password to access unauthorized resources.

- The effects of viruses, worms, and other types of malicious software may be partially mitigated by ensuring access to the file system and registry is restricted.

GE used templates from the NSA (W2k Workstation.INF) and the Center for Internet Security (CIS) (Win2kProGold_R1.2.3.inf) as baselines for workstation security. Some important elements of the Workstation Security Policy are described below.

Security Element	Enhancement/Description
Account Policies Computer Configuration/ Account Policies	▪ Secure Account Policies, consistent with those defined at the domain level, are implemented for local logons. Kerberos Policy is not defined. ▪ Protecting the integrity of local accounts is important. Powerful local users could install unauthorized tools or access company data.
User Rights Computer Configuration/ Local Policies/ User Rights	▪ GE avoids giving users local administrative privileges when possible. All User Rights are assigned only to Administrators accept for the following rights, which are also assigned to Authenticated Users are noted below. Many of these User Rights are described in greater detail in the "Default Domain Controllers Policy" section. ➢ Access this computer from the network ➢ Bypass traverse checking ➢ Log on locally ➢ Remove computer from docking station ➢ Shut down the system
Security Options Computer Configuration/ Local Policies/ Security Options	▪ The company also configures the Security Options for workstations. This helps to further secure the workstations. ▪ Selected values for Security Options are listed below. Many of these Security Options are described in greater detail in the "Default Domain Controllers Policy" section. ➢ Additional restrictions for anonymous connections: No access without explicit anonymous connections ➢ LAN Manager Authentication Level: Send NTLMv2 response only\refuse LM & NTLM ➢ Secure channel options (Secure channel: Digitally encrypt/sign secure channel data always/when possible) are set to values consistent with the domain controllers

Security Element	Enhancement/Description
File System Access Computer Configuration/ File System	▪ GE implements custom NTFS permissions at the workstation level. ▪ Permissions on the root drive of the workstations disk are set to permit Administrators and SYSTEM: Full Control, Authenticated Users: Read and Execute, List Folder Contents, and Read. ▪ Permissions on the Program Files folder, SystemRoot (i.e., \winnt) folder, and the SystemDirectory (i.e., \winnt\system32) are more secure. Administrators and SYSTEM: Full Control, Authenticated Users: Read and Execute, List Folder Contents, and Read.
Registry Access Computer Configuration/ Registry	▪ The CIS security template used has numerous registry permissions defined. GE has not altered the default template permissions. ▪ The registry permissions defined help secure most important keys such as HKLM\software and HKLM\system. ▪ The permissions assigned to most keys allow Full Control to the "root" level key to Administrators and SYSTEM, while those groups and CREATOR OWNER have Full Control on Subkeys. ▪ Registry permissions allow Authenticated Users Read and Execute permissions in most cases.

General Server Security Policy

Member servers such as file servers and DHCP/Print servers also have security configurations enabled through Group Policy. GE used guidance from the NSA ((W2k Server.INF) as well as CIS (W2kSrvGold_R1.0.inf) to develop the baseline standards for member servers. In general, the configuration mirrors the configuration described in the "Default Domain Controllers Policy" section. Thus, specific GP parameters will not be discussed here. The General Server Security Policy helps to improve security by:

- Enforcing strong password and account lockout policies on member server local accounts;
- Enabling the auditing of events that occur on member servers;
- Ensuring event log parameters are adequate to hold audit data and prevent attackers from over writing important audit events;
- Disabling system services that are not used by any member servers; and

- Securing the file system and registry by limiting the groups that are able to have full control over registry keys as well as important files and folders.

Other GIAC Enterprises Information Security Initiatives

GE has other security requirements that cannot be directly addressed solely through technological means such as hardening Windows servers or applying additional group policies. These requirements relate to areas such as how the company recovers from IT failures, manages changes to the systems environment, and addresses security breaches. This section provides an overview of GE's Information Security Program and a summary of key IT processes.

Information Security Program

GE's Information Security Program (ISP) articulates why information security is important and what the company does to ensure appropriate safeguards are in place to protect the confidentiality, integrity, and availability of systems and data. Technology is just one component of a successful information security strategy. A successful strategy is primarily dependent upon the consistent application of appropriately defined policies and procedures by trained individuals who are aware of their roles and responsibilities regarding information security.

The company's ISP is important because it:

- Defines the roles and responsibilities for all employees regarding information security;
- Establishes authority for the Information Technology, Human Resources, and other groups within the company to establish proactive measures to enforce information security policies;
- Sets expectations for appropriate use of IT resources and defines penalties for inappropriate use of company systems and data;
- Helps establish a legal basis for the ongoing monitoring and review of company and user communications; and
- Identifies and articulates the need for important security initiatives and processes, including but not limited to:
  - Security administration (adding, modifying, and removing access),
  - Periodic security audits,
  - End user training and awareness programs,
  - Change control and configuration management
  - System and application auditing and monitoring,
  - Patch management,
  - Intrusion detection and incident response,
  - Privacy management,
  - Data backup,
  - Business continuity management strategies, and
  - Vulnerability management.

Summary of Key IT Processes

Some of the IT processes implemented by GE to help manage business and technology risks are summarized below.

- *Data Backup and Storage Management:* GE's processes that help to ensure complete and secure backups of systems and data exist. The company utilizes the services of a third-party who transports tape backups offsite to a secure storage facility on a daily basis. Every quarter, the IT staff restores certain servers from tape to help ensure backups can be used to restore systems and data after a hardware or software failure.

- *Intrusion Detection and Incident Response Management:* The processes used by the company to detect security events that may be indicative of intrusion attempts, determine if a security incident has occurred, and the associated procedures to follow when a security incident is detected. GE has implemented numerous preventive security controls (e.g., restrictive file permissions and privilege assignments). By aggressively monitoring event logs and deploying host based intrusion detection (HIDS) software on key servers in the environment, the company also has monitoring and detective controls that help to provide a balanced approach to security. While the current size of the company does not justify employing a full-time incident response team, the IT staff is aware of their roles during an incident and how to treat compromised servers.

- *Business Continuity/Disaster Recovery Management:* GE has contingency plans and the associated resources in place to ensure it can continue to fulfill its contractual obligations to LED Corporation (and any other future outsourcing customers). These plans help to address the short and long-term reputation and business viability risks it would face in the event of a major business disruption. The company conducts a major test of its recovery capability each year.

- *Change Management:* GE's processes that address how changes (e.g., security patches, service packs, application upgrades, configuration changes, etc.) to network hosts or applications are applied in the production environment. The company requires that each change be formally tested and approved before introducing that change on a production host/application. Changes can significantly impact not only a particular host or application, but also have cascading affects on dependent hosts and applications.

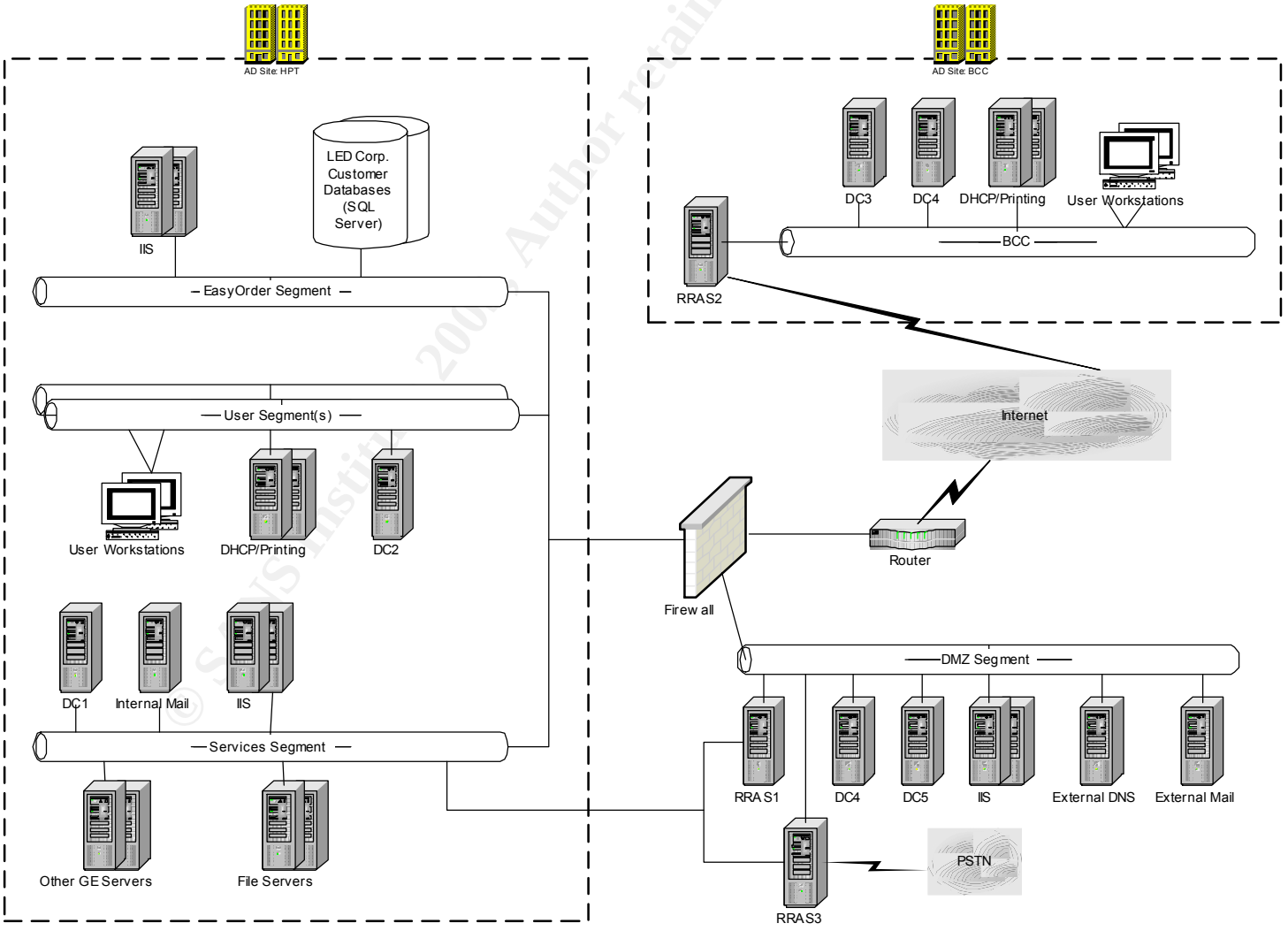
- *Patch Management:* The processes addressing how the company proactively identifies, assesses the applicability of, and schedules testing for, operating system or application patches that are released to address specific security or functionality issues.

- *Data Classification:* GE has defined the types of data that exist within the company, the protection that must be afforded to each data type, and the associated procedures for controlling access based on data type. Roles have been defined within the company that identify the groups permitted to access each category of data.

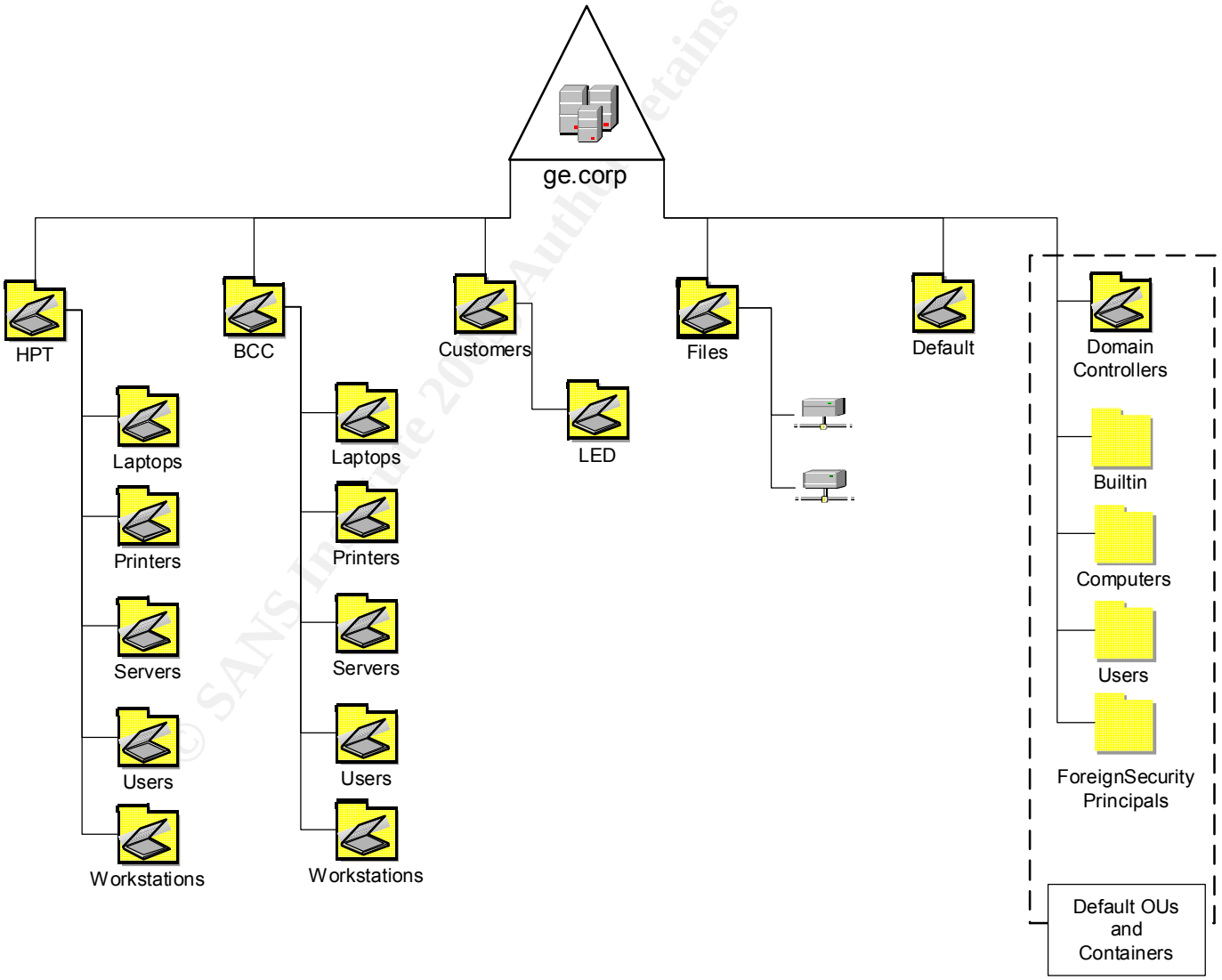
- *Security Administration:* GE's processes that address how system security functions such as granting and revoking access rights, resetting passwords, and issuing IT assets are performed. Standardized processes exist for ensuring access is appropriately authorized, employee terminations are promptly communicated to IT, etc.

- *Privacy Management:* GE transmits, processes, and stores private customer data such as credit card numbers and billing addresses. The company has a responsibility to protect this data from unauthorized disclosure and misuse. GE is aware of the applicable privacy laws and regulations and has taken proactive measures to protect data under its control. The perception of having weak security practices or being subject to privacy litigation are significant business risks.

Appendix A: GIAC Enterprises Network Environment



Appendix B: Active Directory Environment



Works Cited

1. Boswell, William. *Inside Windows 2000 Server.* Indianapolis: New Riders, 2000.

2. Center for Internet Security (CIS). "Level-2 Windows 2000 Server Operating System Benchmark (W2K-Srv.pdf)." 02.2003. <https://www.cisecurity.org/tools2/win2000/W2K-Srv.pdf> (02.23.2003).

3. Defense Security Service (DSS). "DoD Warning Banner." 03.13.2003 <www.dss.mil/infoas/dod_warning_banner.doc> (02.05.2003).

4. Fossen, Jason. GIAC-GCWN Course Materials.

   - *5.1 Windows 2000/XP Active Directory*
   - *5.2 Windows 2000/XP Group Policy and DNS*
   - *5.3 Windows 2000/XP PKI, Smart Cards, and EFS*
   - *5.4 Windows 2000/XP IPSec and VPNs*
   - *5.5 Securing Internet Information Server*
   - *5.6 Windows 2000/XP Scripting for Security*

   The SANS Institute, 2002.

5. Green, Darrin and Brandolini, Shala – Microsoft Corporation. "The Windows Time Service." 04.2001. <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/maintain/operate/wintime.asp> (02.13.2003).

6. Microsoft Corporation. "Active Directory Architecture." <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/ad/windows2000/deploy/projplan/adarch.asp> (11.27.2002).

7. Microsoft Corporation. "DNS Namespace Planning." 02.14.2003. Microsoft Knowledge Base Article – 254680. <http://support.microsoft.com/default.aspx?scid=kb;EN-US;254680> (02.15.2003).

8. Microsoft Corporation. "FSMO Placement and Optimization on Windows 2000 Domain Controllers." 12.20.2002. Microsoft Knowledge Base Article – 223346. <http://support.microsoft.com/default.aspx?scid=kb%3ben-us%3b223346> (02.15.2003).

9. Microsoft Corporation. "Managing Replication Between Sites." From the Windows 2000 Resource Kit Distributed Systems Planning Guide.

10. Microsoft Corporation. Active Directory Sizer Tool. 04.07.2000. <http://www.microsoft.com/downloads/details.aspx?FamilyID=77c0a895-3dfc-469f-be40-6a0ee594821c&DisplayLang=en> (02.08.2003).

11. Microsoft Corporation. "Windows 2000 Server Online Help, Group Policy, Best Practices."

12. Microsoft Corporation. "XADM: Using the Exchange 2000 Sizing Tool." 10.24.2002. Microsoft Knowledge Base Article – 328745. <http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B328745> (03.13.2003).

13. Mills, D. "RFC1769: Simple Network Time Protocol." 03.1995. <ftp://ftp.rfc-editor.org/in-notes/rfc1769.txt> (02.13.2003).

14. National Security Agency (NSA). "NSA/SNAC Router Security Configuration Guide." 02.10.2003. <http://nsa2.www.conxion.com/cisco/guides/cis-1.pdf> (02.13.2003).

15. National Security Agency (NSA). "Windows 2000 Security Recommendation Guides and INF Templates." 05.2003. <http://nsa2.www.conxion.com/win2k/download.htm> (11.25-2002 through 03.15.2003).

16. Nielson, Morten. *Windows 2000 Server Architecture and Planning.* Arizona: Coriolis Group, 1999.

17. Redmond, Tony. "The Importance of the Global Catalog." 02.2001. <http://www.exchangeadmin.com/Articles/Index.cfm?ArticleID=16374> (02.19.2003).

18. The SANS Institute. "The Top Twenty Most Critical Internet Security Vulnerabilities (v. 2.504)." 05.02.2002. <http://www.sans.org/top20/top20_oct01.php#_Toc526136814> (02.05.2003).