Global Information Assurance Certification Paper

GIAC Security Risk and Policy Assessment

GIAC Information Security Officer Training (GISO)
Basic Practical Assignment
Version 1.2 (February 9, 2002)

Prepared by:
Deborah A. Snyder

Submitted March 31, 2003

ABSTRACT

GIAC Enterprises (GIAC) is a small, but growing training services organization. Their primary mission is supporting efficient state and local government services through office productivity training and educational resources.

The purpose of this paper is to provide an overview of GIAC's business model, business operations, information technology infrastructure and how these components support GIAC's business. The document will also discuss security requirements and risks related to protecting the accessibility, confidentiality and integrity of GIAC's critical assets, identifying their top three security risks and providing reasons why each of these is significant, along with recommendations to mitigate same. A review of an existing security policy that addresses one of these high-risk areas will also be evaluated, based on sound policy guidelines and GIAC's needs, and a revised security policy presented that more accurately addresses their security requirements. Finally, based on the security policy identified, security procedures related to the revised policy will be outlined.

SECTION 1

This section provides an overview of GIAC enterprises, describes their IT infrastructure, and describes their critical business operations and IT needs.

Description of GIAC Enterprises

GIAC is a training consultant organization that provides a variety of office automation and tailored application training design, development and delivery services to state and local government agencies. GIAC specializes in program and systems computer-based training and curricula development and delivery, and is dedicated to improving the state of government and community services delivery through education and training. GIAC services encompass performing customer-specific training needs assessments, curriculum planning, training program design, development and testing, production of courseware media and support materials, registration, scheduling and implementation of courseware solutions and follow-up evaluation.

What sets GIAC apart in the market is their ability to effect rapid customization of training curriculum and deliver courseware tailored purposely to meet customers' business needs. To reduce their concept-to-delivery cycle time, GIAC has established relationships with industry standard curriculum vendors, such as Element K[1]. Through these partnerships, GIAC is able to purchase and

[1] Element K Press. "Courseware," 1997-2003 (cited 31 January 2003); available at http://elementkcourseware.com/basics/home.jsp

download quality courseware at negotiated bottom-line prices. GIAC also reaps the benefits of Element K's experience and valuable research in cognitive psychology and instructional design methodologies. This key strategic partnership enables GIAC to utilize off-the-shelf courseware as a foundation, and through targeted assessment and requirements definition, accelerate the development of customized training programs, courseware and instructional materials specifically tailored to their customers' needs and training budgets.

GIAC is organized into five functional departments:

Administrative Services

This department includes the core administrative support operations required to keep GIAC running, including Human Resources, Policy, Legal Counsel, Contract Management, Fiscal Accounting, Audit and Quality Control and Administrative Support.

Planning and Assessment

This department includes the project management and planning specialists, responsible for working with customers to define and manage project scope, goals and objectives, cost and duration, conduct needs assessments and define content requirements, training methodologies, delivery media and testing/evaluation protocols.

Curriculum Design & Development

This department includes the education and curriculum development specialists, programmers and technical writers responsible for training program design, courseware and instructional materials, application development, testing and quality assurance, and courseware documentation and implementation manuals associated with individual training projects and deliverables.

Scheduling and Delivery

This department includes the training program managers and instructors directly responsible for the deployment of the training programs and services and running the training lab. It also includes web design and publishing resources assigned to administer GIAC's web site content and Electronic Registration and Scheduling (ERS) application interface.

Information Technology (IT)

This department is staffed by a combination of GIAC employees and consultants, who provide both internal and external network operations support. Staff also operate and maintain the systems developed and

deployed by GIAC, provide desktop and lab support, network maintenance and monitoring, security management services, inventory and software licensing control.

IT Infrastructure

The IT infrastructure of GIAC is located within its offices in Saratoga, NY. All internal network connectivity is contained within this physical plant and supported by Category 5 cable throughout the location.

Internet connectivity is provided by a local Internet Services Provider (ISP) through two (2) leased fractional T1 broadband lines (different points-of-presence to assure reliable connectivity) and redundant DNS services. These services also enable virtual private networking (VPN) connectivity secured through the Cisco border router and firewall. GIAC relies on the ISP for external Domain Name Server (DNS) functionality to avoid the overhead associated with a split DNS structure.

GIAC has a high level of dependency on IT infrastructure to support their business and limited resources. To enable GIAC to maintain costs, direct available revenues into business initiatives and maximize return on investments, the CEO has directed IT to standardize their technical environment wherever possible. He also directed that IT avoid the lure and risk of cutting edge products in favor of more reliable platforms, operating systems and products from known vendors, to maintain a more stable, manageable and secure environment.

Current network hardware standards include Cisco firewalls, routers, switches and integrated VPN client, Dell servers and workstations, Xerox DocuCenter and Lexmark Optra networked printers. GIAC's prevalent reliance of Cisco products enabled greater integration, ease of security management, and provided support and purchasing leverage.

GIAC recently completed a planned migration to the Windows 2000 operating system and employs the use of central group policies through Active Directory. The decision to move to Active Directory (AD) was based on the fact that it supported a centralized, automated approach to management of user data, security and distributed resources. AD also integrates DNS/Dynamic DNS at workstation level to support efficient communications within the intranet. Procurements are reviewed by IT and must be Windows 2000 compatible. Variations are not permitted unless approved and authorized.

GIAC's network is relatively straightforward in design (refer to Diagram 1), with limited points of external connectivity. Its multi-tiered architecture supports a "Defense in Depth" strategy to protect resources from external and internal threats. This layered approach to security helps decrease the likelihood that the failure of one security mechanism will lead to the loss or compromise of network resources and/or information. The network was configured based on GIAC's

business and security requirements, and follows standards set forth in Cisco's SAFE Security Blueprint.[2]

External Gateway

A Cisco 1710 Security Access border router running Cisco Internetwork Operating System (IOS) 12.x secures GIAC's network outer perimeter. The router's primary job is to direct packets between the Internet to the DMZ, however, this component is configured to do more than simple routing. It integrates multiple functions including advanced routing, stateful inspection firewall, intrusion detection (IDS) and high-performance virtual private network (VPN) functions. As configured, the router's features help assure secure Internet, Intranet and extranet access, and comprehensive security screens the architecture of GIAC's internal network from the outside world, safeguards data and protects internal network resources from unauthorized access. Services and applications include:

- Cisco IOS Software.
- Network Address Translation (NAT)/Port Address Translation (PAT) is used to provide network addressing efficiency and hide private address space.
- Virtual Private Network (VPN) functionality using the integrated VPN client, supports remote user access to network resources. Strong authentication and hardware-based encryption increase the security of this access point.
- The router was configured at installation based on Cisco technical documentation and implementation guides[3] and third party professional consultant guidance. The security policy applies a deny by default philosophy in that it is tuned to only allow required network services between GIAC's network and the Internet, and deny everything else.
- Access Control Lists (ACLs) are in place to filter all traffic as it passes through, and permit or deny packets based on the rules set. Router filters are configured to block anything that would be denied at the firewall gateway, adding an early warning layer to detect potential network scan attempts, help reduce risk and shorten detection and reaction time. IP filtering and port filtering protects the firewall from evaluating unnecessary traffic. SNMPd, FTPd, telenetd and other vulnerable daemons or unused services are disabled. The router is also configured to recognize and block known attacks (I.e., IP spoofing). Traffic to the web server within the DMZ is limited to web traffic (HTTP and SSL traffic to ports 80 and 443 from the Internet to the web server). All packets originating at the web

[2] Cisco Systems, Inc., "SAFE Blueprint for Small, Midsize, and Remote-User Networks," 2001 (cited 5 January 2003); available at http://www.cisco.com/en/US/netsol/ns110/ns129/ns131/ns128/networking_solutions_implementation_white_paper09186a008009c8a0.shtml

[3] Cisco Systems, Inc., "Cisco 1710 Series Access Routers, Technical Details," 2003 (cited 17 February 2003); available at http://www.cisco.com/en/US/products/hw/routers/ps221/prod_technical_details.html

server are blocked except outgoing HTTP or SSL *in response* to outside requests.
- The router also incorporates authentication and encryption protocols to assure secure access into GIAC's network.
- CiscoWorks2000 Web-based network management suite is used for remote monitoring, administration and troubleshooting.

Authentication

Authentication involves taking an identifier, and combining it with some other piece of information that is unique to the identifier and that only that individual would know.[4] In private and public computer networks (including the Internet), authentication commonly involves the use of logon passwords. GIAC employs password-based security to control access to systems and information. One-factor authentication through the use of logon passwords (user ID and a password) is used for both internal and external access authentication.

As the inherent weaknesses of one-factor authentication are well understood, IT places particular importance on granting access permissions based on the Principle of Least Privilege[5], permitting only minimum access, for the period required, by individuals to accomplish their assigned job duties. Although it creates overhead, IT implemented policies and procedures regarding this access control principle for both internal and external access. Management and supervisors are responsible for assuring that employee and consultant roles and responsibilities are aligned with access permissions, and reexamined whenever an individual's job changes or they relocate to another department. It is a known fact, however, that supervisors often simply request full access or request access permissions that match existing employee profiles, rather than actually analyzing and defining access needs based on an individual's role and responsibilities. Access permissions are rarely reexamined when employees' duties change and there are often delays in reporting when employees or consultants leave GIAC so that access can be promptly terminated. These practices limit IT administrators' ability to manage user profiles and control access to networked resources.

DMZ

Two External Internet Cisco PIX 515 firewalls running PIX OS version 6.3, are clustered at the gateway to the DMZ, to provide high availability, load balancing and fault tolerance through automatic failover capabilities. Firewalls configurations were based on Cisco technical documentation and implementation

[4] SANS Institute, GIAC Information Security Officer Training, Track 9, Terms and Concepts Part 5, 2003 (cited 22 February 2002), p. 1-16.
[5] SANS Institute, p. 1-27.

guides[6] and third party professional consultant guidance. Services, applications and rules include:

- PIX Device Manager (PDM) Version 3.0.
- Open Shortest Path First (OSPF) provides dynamic and efficient routing and Cisco PIX Firewall NAT services ensures secure routing through tight integration with Network Address Translation (NAT) to provide private IP addressing to the internal network.
- Firewall rule sets or Access Control Lists (ACL) based on GIAC's security policy and requirements were established by the third party consultant at the time of original installation. Subsequent updates to the rule set have been documented and managed through a change control process. The ACLs were designed to support GIAC's business and security needs. For example, all internal outbound services from the internal network are allowed, but unnecessary services are eliminated. Firewall access is locked down, but permits access by firewall administrators. Internet and internal users have SMTP access to the mail server and HTTP access to the web servers. Rules limit traffic to the web server within the DMZ to HTTP and SSL from the Internet to the web server. Packets originating at the web server are blocked. Only outgoing HTTP or SSL in response to outside requests are permitted. Systems in the DMZ cannot initiate connections to the internal network. Packets that do not meet firewall rules are dropped. The firewall also provides protection from popular forms of attacks including Denial-of-Service (DoS) attacks and malformed packet attacks performs TCP and IP packet validation, URL filtering, content filtering, stateful inspection and virtual packet reassembly, searching for attacks that are hidden over a series of fragmented packets.
- Web content filtering is provided through Websense integration.
- Integrated IDS intrusion detection and protection features include the use of DNSGuard, FloodGuard, FragGuard, MailGuard, IPVerify and TCP intercept, and monitoring for known attack "signatures." IStrong integration with Cisco Intrusion Detection Systems (IDS) sensors enables the firewalls to automatically block hostile network nodes.

Internet and Web Mail Servers

Outlook Web Mail Access is provided through a Dell PowerEdge 1600SC dual processor Xeon server running Windows 2000 Server, Service Pack (SP) 3. Applications and services include Microsoft Exchange 5.5, Antigen AV and 2 scan Engines (McAfee and Norton).

[6] Cisco Systems, Inc., "Cicso PIX 500 Series Firewalls" 2003 (cited 15 February 2003), available at http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/prod_technical_details.html

Internet Web Site Services are supported through a Dell PowerEdge 1600SC dual processor Xeon server running Windows 2000 Server, SP2. Applications and services include Internet Information Services (IIS) 5.0, SP2, GIAC marketing and services content, GIAC's Course Registration and Scheduling application (interface only) and Norton AV.

Intrusion Detection

Intrusion Detection System software and hardware is in place to monitor both the DMZ and internal network for abnormal activities (Cisco IDS 4210 running Cisco Secure Intrusion Detection System software version 4.0). It provides intrusion detection monitoring for both DMZ and Internal network, including packet sniffing and anomalies analysis, extended threat detection and classification capabilities, stateful pattern recognition as well as protocol and traffic anomaly detection. Cisco Secure Scanner is used periodically to ensure firewall configurations are functioning as intended and that IDS alarms are operating to ensure security across the network.

Firewall Management and IDS Station - Dell, Pentium 4 Processor, 1.8 Ghz with 256 Mb RAM, 20 Gig Hard drives, running Windows 2000, Service Pack 3. Applications and services include PIX Device Manager (PDM) Version 3.0, Cisco IDS Device Manager, IDS Event Viewer, CiscoWorks VPN/Security Management Solution (CiscoWorks VMS) and Norton AV.

Intranet

Two Cisco PIX 500 firewalls running PIX OS version 6.3, are clustered at the gateway to GIAC's the Intranet. Services, applications and firewall configuration details are essentially the same as the two firewalls above. Firewall rule sets (ACLs) were designed to provide additional controls and protections for the Intranet based on Cisco technical documentation, implementation guides and third party professional consultant guidance.

A Cisco Catalyst 3550 12T router running Cisco Internetwork Operating System (IOS), and three Cisco Catalyst 2950 Series fixed-configuration Fast Ethernet switches running Cisco Internetwork Operating System (IOS) manage GIAC's internal subnets and control access to sensitive assets such as contract and financial data, employee information and proprietary software.

Services and applications on the router include Cisco Cluster Management Suite (CMS) Software and Network-wide services, advanced QoS, rate-limiting, security access control lists, multicast management, and high-performance IP routing, and maintain traditional local area network (LAN) switching simplicity.[7]

[7] Cisco Systems Inc., "Cisco Catalyst 3550 Series Switches," 2003 (cited 19 February 2003), available at http://www.cisco.com/en/US/products/hw/switches/ps646/products_data_sheet09186a00800913d7.html

The internal switches employ ACLs developed based on Cisco technical documentation[8], the Catalyst 2900 Series Configuration Guide[9], and third party vendor consultants guidance at implementation. Enhanced Image (EI) Software provides rate limiting and security filtering services. VLANs limit forwarding of packets to stations defined as part of the VLAN and provide security barriers between end stations connected through the same switch. An External Redundant Power Supply (RPS) assures network high availability.

Antivirus Protection

Anti Virus software is installed on every workstation and server (Norton Corporate, Antigen on Exchange server). Virus definition files are kept current through a managed parent server distribution process. Symantec™ AntiVirus Gateway Solution and TrendMicro Virus Wall are being evaluated to provide additional virus and malicious code protection at the Internet gateway for Web (HTTP), file transfer (FTP), and email (SMTP) traffic. These solutions are being considered based on their abilities to protect against email viruses, block SPAM and guard the network against blended threats.

Servers

GIAC's server environment contains a mixture of Dell PowerEdge and PowerVault models. Individual details for each server within the intranet are provided as follows:

GIAC Research and Development Server - Dell PowerEdge 1600SC dual processor Xeon server, with redundant SCSI hard drives, running Windows 2000 Server, Service Pack (SP) 3. Applications and information resources within in this research and development environment include Element K curriculum libraries, development versions of GIAC's training courseware applications, testing software and databases and Norton AV. These components are partitioned and use mirrored drives to effect automated backup runs nightly.

GIAC Production Server - Dell PowerEdge 1600SC dual processor Xeon server, redundant SCSI hard drives, running Windows 2000 Server, SP3. The applications and services on this production environment include GIAC's Proprietary Training Courseware Applications, Registration and Scheduling application, shared project management, contract monitoring and reporting applications and Norton AV. These components are partitioned and use mirrored drives to effect automated backup runs nightly.

GIAC Database Server - Dell PowerEdge 1600SC dual processor Xeon server, running Windows 2000 Server, SP2. This server hosts GIAC

[8] Cisco Systems Inc., "Cisco Catalyst 2950 Series Switches," 1992-2003 (cited 17 February 2003), available at http://www.cisco.com/en/US/products/hw/switches/ps628/prod_technical_details.html
[9] Cisco Systems Inc., "Catalyst 2900 Configuration Guide," 1992-2003 (cited 17 February 2003), available at http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2900/index.htm

employee, customer, contract and scheduling registration databases. Applications and services: Microsoft SQL Server 2000, SP2 and Norton AV.

ISA (Proxy) Server - Dell PowerEdge 1600SC dual processor Xeon server, running Windows 2000 Server, SP3. Applications and services: Microsoft ISA Proxy Server 2000, GFI DownloadSecurity for ISA Server (previously LanGuard) for web content filtering and AV, GFI LANguard Network Security Scanner and Norton AV.

Active Directory (AD)/DDNS DHCP Servers - Dell PowerEdge 1600SC running Windows 2000 Server, SP3. Applications and services: Microsoft Active Directory Server and Dynamic DNS Server functionality and Norton AV.

File/Print and AV Updates Server - Dell PowerEdge 1600SC, running Windows 2000 Server, SP3. Applications and services: Microsoft File/Print Server functionality, Norton AV and Server update management software.

Internal Mail Servers - Dell PowerEdge 2100, running Windows 2000 Server, SP 2. Applications and services: Microsoft Exchange 5.5, Antigen AV and 2 scan engines (McAfee and Norton).

Centralized Backup Server - Dell PowerVault 132T SDLT 320 Tape Library for server, LAN and SAN backups. Applications and services: VERITAS Backup Exec 9.0 for NetWare and Norton AV.

RADIUS (AAA) Server - Dell PowerEdge 1600SC dual processor Xeon server, running Windows 2000 Server, SP3. The applications and services on this production environment include Remote Authentication Dial-In User Service (RADIUS) software, authentication, authorization, and accounting (AAA) network security services to control access to requested systems and or services, and Norton Corporate AV.

Workstations and Laptops

Workstations are a mixture of newer Dell Pentium 3 and 4 devices, and a few older, less reliable CSS Labs – Pentium 2 models. All are running Windows 2000 operating system, SP2 or SP3, Microsoft Office Professional 2000, IE. 5.0 with SP2 and Norton AV.

Dell Laptitude laptops are used by administrators and instructors for remote access. These devices have essentially the same software as the Dell workstations described above and a Cisco VPN client to provide secure remote access.

Security settings follow the guidance provided in the National Institute of Standards and Technology (NIST) Systems Administration Guidance for

Windows 2000 Professional[10] and Windows 2000 Gold Standard, a minimum security standards jointly developed by the Center for Internet Security, National Security Agency (NSA), (NIST), the SANS (SysAdmin, Audit, Network, Security) Institute and others. Baseline security setting checklists and templates allowed GIAC administrators to configure workstations to a high level of security.

General

A recent network assessment conducted to determine scalability and security, identified several vulnerabilities and opportunities for risk mitigation.

IT procedures require that all hardware and software patches and fixes and service packs, on all components be kept up-to-date, however, this poses a challenge and administrators have reported they are not able to keep up.

While the infrastructure exists to support it, data and systems backup procedures are not consistently performed in a routine and scheduled manner. There have been several recent instances where critical files and data have been lost and could not be recovered.

While experienced and dedicated, GIAC's IT resources are spread thin across many critical tasks and responsibilities, and they are dealing with a rapidly evolving environment as GIAC expands and implements new ways of doing business. Too often, competing projects and tasks compromise effectiveness and force hard choices as to what can be done with available resources. GIAC has no Security Administrator on board, and none of the IT staff come from an information security discipline, consequently it has been a struggle to balance security concerns with operational tasks. In some areas, the expertise required to design and implement secure components and rule sets exceeds existing staff skills and experience.

[10] National Institute of Standards and Technology, "NIST Systems Administration Guidance for Windows 2000 Professional - Special Publication 800-43," 2002 (cited 20 December 2002); available at http://www.csrc.nist.gov/itsec/guidance_W2Kpro.html#NIST_W2K

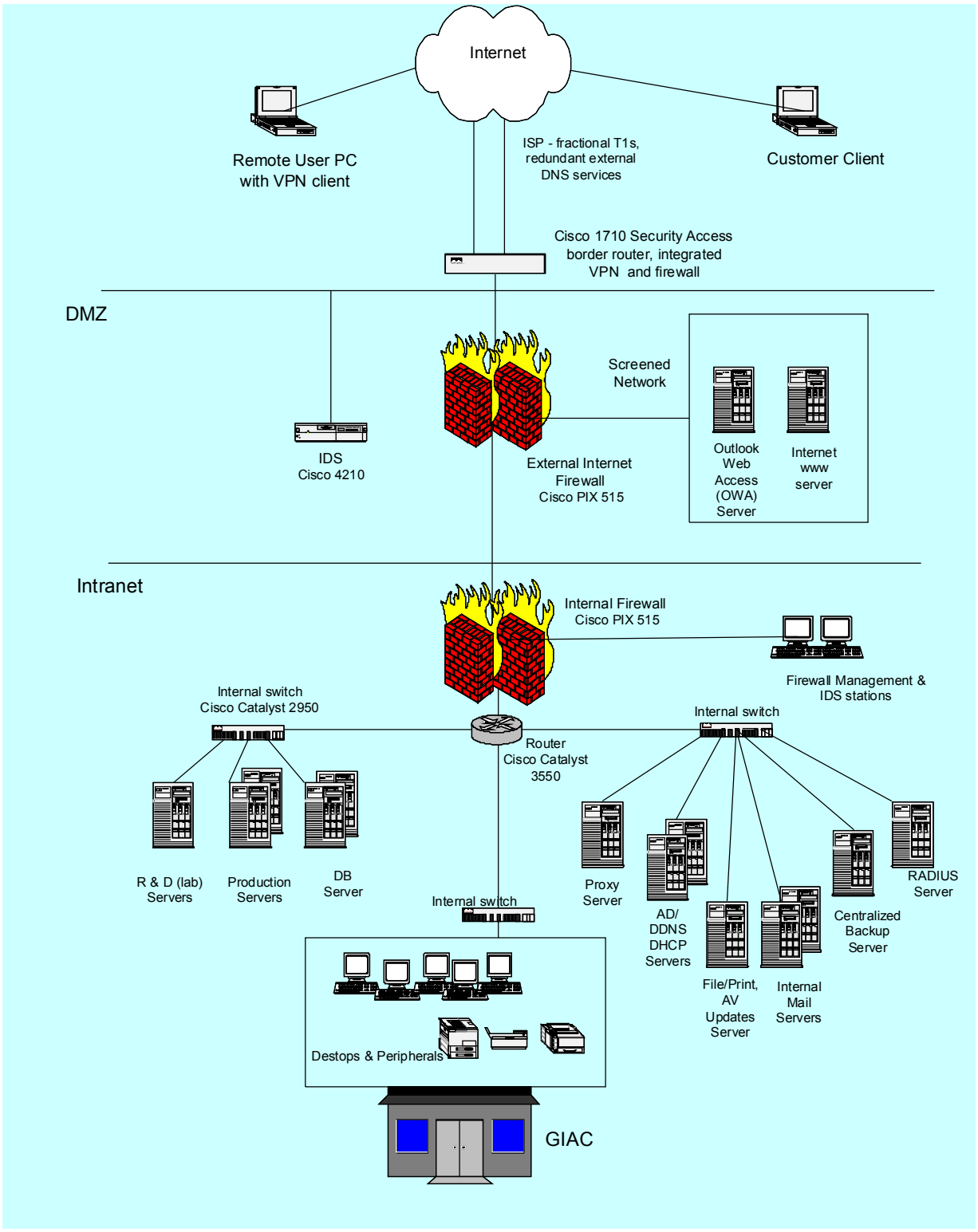

Figure 1 – *GIAC Network Diagram*

Business Operations

GIAC's growing reputation is based on their ability to rapidly customize training and deliver courseware tailored to meet customers' needs. GIAC's continued success and capacity to grow their business will depend on their ability to expand products and services marketing, sustain and improve upon their concept-to-delivery cycle time, increase functionality available through the Internet, keep costs down, and maintain their reputation for delivering quality instructional materials that produce exceptional results.

GIAC's key business operations include the ability to conduct training needs assessments, define and produce customized courseware, manage contracts and projects, communicate effectively and efficiently internally and with partners, and customers, market products and services, support course registration and scheduling through a secure and highly available website, and distribute and deliver training programs to meet their customers' needs and expectations.

The work GIAC performs is heavily IT-dependent. Every department to a large extent, depends on email, Internet access, office productivity software, access to courseware, scheduling and registration interface and databases, and various other system resources and information to keep GIAC's business operations flowing and accomplish routine tasks.

GIAC's critical operations depend most heavily on reliable access to and protection of the development, production and database servers that support their training courseware libraries, courseware development and training applications. These resources are critical to supporting GIAC's customized development and delivery work processes, and are therefore considered their "crown jewels." Access is limited to internal use only. Assuring the accessibility, integrity and confidentiality of these key resources is of the utmost importance.

To protect their business relationships, courseware source code purchased from vendors, GIAC's proprietary courseware, training programs and materials, and customer-related data must be safeguarded from unauthorized access, use, theft and/or damage. Insufficient risk management and quality control in these areas could result in loss of reputation, relationships and/or partner goodwill, customer dissatisfaction and would no doubt negatively impact revenues, repeat and referral business, and short and long-term business expansion plans.

GIAC also depends heavily on high availability and security of their Internet web site to market products and services, and support customer and trainer access to their online Electronic Registration and Scheduling interface. Reliable external access by customers researching their products or registering and scheduling courses is critical. Course Instructors require secure external access to these and other resources to support their client site activities and informational needs. GIAC staff also require internal access to the site and background customer and

training registration and schedule databases to administer and track training projects and deliverables.

All functional areas require reliable access to supporting business components such as email, contract and project management tracking software, administrative applications and networked files. Email is vital to efficiently and effectively and communicating and sharing information with partners, customers and remote users. Efficient communication and exchange of information between GIAC's functional departments is key to efficiency and quality. Project and contract management applications enable GIAC to effectively manage multiple contracts and projects. All GIAC employees use Microsoft office automation and email software (Outlook, Word, Powerpoint, Excel, Access). In some instances staff only require access from within the GIAC internal network. In other instances, course instructors and managers working offsite require remote access (I.e., from a customer site, hotel or home) to courseware, email, databases and other network resources located on the GIAC internal network, as well as access to the Internet. This business requirement is supported via secure VPN access.

The network resources and information assets that support these operations are crucial to GIAC's business operations and key to their ability to provide faster and better service than their competitors. The accessibility, integrity and confidentiality of these systems, applications and data must be prudently assured and securely protected. Maximum availability, failsafe backup, reliable restoration procedures and redundancy in these critical areas is essential to safeguard and assure reliable access to these "crown jewels". Without these assets, GIAC's work progresses would virtually and literally come to a standstill, as there are few areas where manual processing alternatives are available or would prove an adequate replacement.

The CEO recently issued an aggressive five-year strategic plan that focuses on assuring business, market and financial growth objectives. The plan includes extension of training delivery methods to the Internet through a secure GIAC e-Learning Portal (ELP). This transition is expected to reduce instructor and trainee travel costs and training time, and enable GIAC to reach a wider audience. The plan also included technology enhancements and recommendations regarding improvement in known security risk areas. In implementing this strategic plan, management must assure the following:

1) GIAC's training programs must assure they maintain the same standards of excellence and customer satisfaction that the company has built their reputation on;
2) Standardization should be implemented wherever possible to simplify processes, aid integration, ease of management and reduce costs;
3) Proper consideration of information security must be assured at all levels to protect GIAC's assets; and,

4) All initiatives and investment proposals must be reviewed by GIAC's centralized project office to determine if they meet pre-defined project portfolio criteria designed to assure alignment with the strategic plan and bring value to the business.

The CEO and management are cognizant of the relationship between planned business redesign and growth initiatives, and expansion of the GIAC network infrastructure to support increased business, new functionality and methods for conducting business. They understand that as your IT infrastructure grows, so does its complexity.[11] What they may not recognize is that there is a correlation between network complexity and information security risk, and that information security must be viewed as a valuable and sound business investment.

SECTION 2

This section identifies the areas of risk that are most critical given the nature of GIAC's business, and discusses these risks in the context of GIAC's business requirements and interest in assuring the protection of critical information assets.

Critical Assets

GIAC's network, computers, communication devices and the information stored or processed on them represent major capital investments. Like many other companies, GIAC relies heavily on critical information assets to perform their mission and achieve business goals. GIAC's business and ongoing ability to provide faster and better delivery of services than their competitors' depend on the following critical processes, information and infrastructure components:

- Proprietary vendor and GIAC courseware and development process;
- Electronic Registration and Scheduling (ERS) web-based application interface and background databases; and,
- Email, shared business productivity applications and files that enable GIAC to efficiently conduct business and maintain communications with customers and between GIAC's functional departments.

Risk Assessment

The risks and consequences of inadequate information security and integrity can be operational, financial, legal and political, and can include:

- Loss or corruption of critical information and/or intellectual property;

[11] Bitpipe Inc., "Return to Business Value - Gaining ROI from Enterprise System Management," 2002 (cited 31 January 2003); available at http://www.bitpipe.com/data/detail?id=1036096051_748&type=RES&src=FEATURE_RESTRM&x=1888050311

- Lost business, fiscal assets or decreased performance due to downtime, such as the disruptions of service experienced with the Nimda virus and recent SQL Slammer worm;
- Direct or indirect decline in revenues or market share;
- Lost or reduced customer/constituent/partner confidence;
- Damage to the organization's image and reputation;
- Compromised privacy/confidentiality;
- Potential federal/state privacy of information non-compliance and penalties; and/or,
- Criminal or civil lawsuits, associated litigation costs and damages to injured parties as a result of litigation.

The best protection against inappropriate access, misuse and debilitating attacks on business information assets is to know where your vulnerabilities and risks lie.

Risk is a function of the likelihood of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization.[12]

Establishing the value of critical information assets and performing a risk assessment helps determine risk areas and gaps in information security protocols. Risk analysis allows an organization to bring their information security concerns into focus. Understanding threats, risks, available mitigation options and associated cost benefits is a critical first step in developing a sound security plan. Risk assessment, while still a young science, with a certain amount of craft involved, has proven itself to be very useful in helping management understand and cost-effectively address the risks to their information and IT environments.[13]

The risk assessment methodologies GIAC used were based on current industry best practices. A process known as an Annual Loss Expectancy or Exposure (ALE) was used. The ALE takes the value of an asset and then the likelihood of a threat occurrence in a formula to calculate the ALE: the asset value (V) multiplied by the likelihood (L) of the threat (V x L = ALE)[14].

GIAC's Baseline Risk Assessment and Analysis report identified the risks and threats that pose the greatest potential impact on their critical assets and business operations over time. This provided management with insights that helped shape and implement a security plan to address priority areas first, along with a baseline for future comparison. Risk areas that could be resolved easily, at little or no cost, but if addressed would improve overall security (low hanging

[12] National Institute of Standards and Technology, "Risk Management Guide for Information Technology Systems – Special Publication800-30," 2002 (cited 2 December 2002); available at http://www-08.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

[13] Harold F. Tipton, Micki Krause, Information Security Management Handbook, 4th Edition, (Boca Raton 2000), p. 258.

[14] Will Ozier, Risk Assessment and Management, Data Security Management, (Boca Raton 1995).

fruit), were also given consideration. The assessment also considered existing vulnerabilities, and mechanisms and controls already in place within GIAC.

Performing a risk assessment enabled GIAC to be practical and selective, applying available resources to mitigating areas of highest potential threat, maximizing benefits and return on investment.

Based on the nature of GIAC's business operations, goals and information security requirements, the following risk areas were determined to be most critical:

1. Loss of confidentiality and/or availability due to unauthorized access to proprietary courseware products;
2. Loss of availability or integrity of GIAC's Internet site and web-based Electronic Registration and Scheduling interface; and,
3. Loss of availability of electronic communication capabilities due to hardware failure.

The following three sections explore these specific risk areas in greater detail and present mitigations strategies GIAC can use to control and manage security risk within safe and acceptable levels for their business.

Specific Areas of Risk

1. Risk / Threat

GIAC's critical operations depend most heavily on the development, production and database servers that support their training courseware libraries, courseware development and training applications. Therefore, these resources are considered to be GIAC's "crown jewels."

Loss of confidentiality and/or availability due to unauthorized access to proprietary vendor curriculum libraries and GIAC proprietary courseware presents a serious business risk for GIAC. The proprietary curriculum libraries that GIAC purchases along with the trusted-partner business relationship they have with the supplier, are critical to GIAC's business operations, goals and performance. GIAC's ability to maintain cost-effective development and delivery cycles, meet contractual agreements and provide better services than their competitors' ability relies heavily on the vendor supplied standard curriculum they use as a baseline to expedite delivery of customized training courses and materials.

User licenses associated with this asset includes a contractual obligation to safeguard and protect the proprietary courseware from unauthorized disclosure, access and/or theft by others. Expectations that GIAC will take the necessary steps to safeguard theses valuable assets is intrinsic in their ongoing partnership with the supplier. GIAC's custom-tailored training programs are what sets them

apart from their competitors, enables them to better meet customer expectations and contractual commitments, and maintain a crucial market edge.

These key strategic assets provide the foundation that enables GIAC to accomplish rapid development and delivery of customized, quality training programs for their customers. Access to these assets must be tightly controlled and properly managed to protect against unauthorized access, use, disclosure, damage or loss.

Relevance

GIAC uses password-based authentication to control access to systems and information. One-factor authentication through the use of logon passwords (user ID and a password) is used for both internal and external access authentication. GIAC does not have sufficiently strong password protocols and role-based access controls in place to assure protection of critical information and assets from unauthorized assess.

Appropriate controls on granting access permissions and strong passwords are critical to system security. Account access and password mismanagement can create a myriad of serious security vulnerabilities for an organization. Threats of unauthorized access can come from both inside and outside of the organization. Threat-sources could include hackers, computer criminals, competitors, insiders with insufficient security awareness training or disgruntled, malicious, negligent, dishonest or terminated employees or contractor staff.

While IT has stressed the importance on granting access permissions based on the Principle of Least Privilege, and created policies and procedures regarding this access control principle for both internal and external access, they are not consistently followed or enforced. Management and supervisors often resort to requesting full access or basing access permissions on existing employees' user profiles rather than ensuring access needs are based on an individual's role and responsibilities. Procedures for access review when employees' duties change and prompt reporting when employees or consultant leave GIAC are not followed. As a result, it is difficult for IT administrators to manage user profiles and control access to networked resources, and individuals may have access to information and/or assets they should not have or do not need.

IT has also stressed the importance of strong passwords, issued a password policy and password protection guidelines, however, proper protocols are not always followed. According to Davis, even when formal policies outlining appropriate use exist, many users still take a casual approach toward security.[15]

---

15 Jeff Davis, "Download our posters to raise awareness about IS security," in TechRepublic [electronic newsgroup], (29 October 2002, [cited 17 January 2003]); available at http://www.techrepublic.com/article.jhtml?id=r00320021029jed01.htm&fromtm=e101-3

Employees are focused on routine operational processes and tasks, and often, in the interest of convenience and efficiency, resort to lax everyday password practices that compromise security and present risks to the business.

Users commonly resort to using simple, ordinary words or words with known associations (favorite pet or sports team) in an effort to make them easier to recall. The practice of writing passwords down and sharing them with others is fairly commonplace. Many individuals have multiple passwords to remember and as a result, post or share them, create weak passwords or replicate the same password across all of their accounts to manage them more easily. These practices could result in passwords being compromised and people obtaining access to information and/or access rights and permissions they should not have.

Shared or stolen passwords can be put to nefarious purposes. Compromised passwords also destroy the integrity of audit logs that help identify what actions were carried out, by whom and when. The lack of password complexity and proper password management also increases the potential for a basic password guessing or cracking strategies such as dictionary attacks[16] and social engineering. Social engineering is the process of exploiting humanistic weaknesses such as the desire to help those in need.[17] Social engineering tricks often cause individuals to divulge sensitive information to others who do not have appropriate authorization or become an unknowing participant in an cyber-attack on the organization.

The high probability of insider security breaches is also a relevant factor in examining this threat. Ninety percent of the respondents (corporations and government agencies) to Computer Security Institute's 2002 Survey reported computer security breaches within the twelve-month period surveyed. Eighty percent or more of the security threats and penetrations reported occurred internally.[18]

GIAC is a small company strategically focused on managing costs, reinvesting capital in expansion and growth in market share, while still maintaining their reputation for rapid delivery of quality products and high customer satisfaction.

The risks GIAC is exposed to due to the lack of sufficient controls and users not adhering to policies, procedures and responsible behavior habits in these areas seriously endangers their ability to ensure the privacy and security of

[16] Edward Hurley, "Testing Password Strength Gives Policy Some Bite," in TechTarget Network [electronic newsgroup], (29 October 2002 [cited 17 January 2003]); available at http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci858747,00.html

[17] Jarvis Robinson, "Internal Threat – Risks and Countermeasures," 15 November 2001 (cited 22 November 2002); available at http://www.sans.org/rr/threats/internal.php

[18] Computer Security Institute, "2002 Computer Crime and Security Survey," April 7, 2002 (cited 22 November 2002); available at http://www.gocsi.com/press/20020407.html

proprietary and confidential information, and protect their critical assets and IT infrastructure.

Potential Impact and Consequences

Unauthorized disclosure or release of sensitive information and unauthorized physical or logical access may be gained through failure to implement sufficient authentication mechanisms and properly protect passwords.

A loss of confidentiality due to unauthorized access to vendor supplied curriculum could result in a loss of partner confidence, damaging or even severing the critical relationship with their courseware supplier. The resulting loss of access to these curriculum libraries would dramatically effect GIAC's agility in developing and delivering products and services, their ability to focus on customizing the courseware to customers' business needs, and training courseware quality.

A breach of GIAC's legal obligations in this area could also result in failure to deliver on contractual obligations to their customers, as well as their being held liable if they were found negligent in protecting their partner's proprietary information. Based on a breach of duty in failing to live up to that obligation, the supplying vendor could claim harm, loss of assets and/or business opportunities, resulting in litigation and potential punitive damages against GIAC.

GIAC's customized courseware is their core product line. The quality and flexibility of their delivery system, products and services, and customer satisfaction has kept them ahead of market competitors. Inappropriate access, misuse, deliberate destruction, theft of proprietary information, or disclosure to a competitor could negate this advantage and result in severe losses and impact to their competitive edge.

GIAC has state and local government agencies contracts that are supported by federal funding. Federal statutes such as the Electronic Communications Privacy Act of 1986 and the Federal Privacy Act of 1976 require effective security of computer systems holding confidential information. Failure to meet set requirements and standards to ensure security could result in loss of these contracts and non-compliance penalties.

GIAC has legal obligations associated with contracts and a responsibility to exercise due diligence in protecting assets, employee and customer information. Loss of confidentiality could impact GIAC's ability to meet contractual obligations, and also lead to possible legal actions against GIAC by injured parties seeking damages. Litigation costs and damages could serious affect both their profit margin and corporate reputation.

Mitigation Strategies

The following risk mitigation steps are proposed:

- Review existing access and password controls and policies to ensure they are clear, concise, complete and enforceable. Make changes as required to cover the issues the policy seeks to address and articulate tasks and responsible parties. Update internal procedures and controls to assure policies are consistently implemented and followed. Provide easy access to these security policies & procedures – an intranet web site works well in ensuring all employees can access relevant policy and procedural information they need.
- Work with Departments managers and supervisors to review and ensure each individual's user access permissions are based on their role and responsibilities.
- Consider areas where additional system and application level access authentication and authorization controls can be implemented to enforce policies and provide added protection for these key resources.
- Implement technical mechanisms such as: password filters that check passwords against set criteria (length, combinations of letters, numbers and special characters, previous history, etc.) to ensure users create strong passwords. Require passwords to be changed at regular intervals, disallow use of User ID as password, and employ password lockout and reset count options to control bad logon attempts. Implement Windows policies and controls to password-lock devices after a specified period of inactivity (I.e. 10 minutes), and return a blank logon screen versus displaying the last User ID logged on.
- Consider the feasibility of moving to two-factor authentication, encrypting passwords where they are stored on the system and/or implementing a firewall between critical resources and the rest of the intranet with strict access policies to boost security.
- Monitor and enforce access permission and password policies. Periodically conduct reviews of user access permissions and run password checker or cracker programs periodically to ensure policies are being followed and mechanisms are functioning as intended. Take appropriate corrective action where necessary to reinforce GIAC's security stance.
- Recognize individuals who act in an appropriate fashion. This will serve to reinforce the message that security is everyone's job and encourage others to act similarly.
- Ensure procedures and controls address quick removal/revision of access permissions for individuals who should no longer have access or whose access permissions should be modified due to changes in job duties or clearance levels.
- Create procedures to monitor access accounts and routinely disable/purge User IDs with no activity for a specified period of time.

Due to the 'people factor' involved in these areas, mitigation success in this area will depend on clear and accessible policies, increased awareness, implementation of appropriate technical mechanisms, internal controls and procedures, and ongoing monitoring and enforcement activities.

Implementing an effective training program to increase information security awareness at all levels will further support reducing this risk area by ensuring employees understand the value and importance of the assets protected through these policies and procedures, and their role and responsibilities. It can be relatively cost-effective and still be one of the best investments GIAC can make to improve its overall security stance. Strategies to consider include but are not limited to:

- Remind users on a routine basis that protecting their passwords and assuring information systems security is the responsibility of every employee.
- Provide refreshers on privacy and confidentiality laws, regulations and requirements to reinforce employees' role and responsibility to ensure compliance.
- Keep information security on the radar. Issue awareness updates and related articles in company newsletters, web site or use industry services such as Computer Security Institute FrontLine newsletter, designed to increase awareness in every employee in the organization[19]. Encourage subscriptions to relevant industry periodicals and technical newsletter services such as the SANS Newsletter[20] to increase network/system administrator skills and awareness levels.
- Hold Security Awareness Forums and/or an organization-wide Computer Security Awareness Day in conjunction with National Computer Security Day[21], to raise awareness of information security issues, and provide employees with knowledge and motivation to be proactive participants in GIAC's security plan.
- Use posters, visual displays or daily screen saver tips to reinforce adherence to critical security concepts within the workplace.

2. Risk / Threat

Loss of availability or integrity of GIAC's Internet site and web-based Electronic Registration and Scheduling (ERS) interface due to an attack on their web server presents a serious business risk for GIAC.

GIAC depends heavily on its Internet presence to promote and market their training services and courseware products. The ERS interface supports a primary function within GIAC's business operations. All registration and scheduling activities by customers, field managers and instructors are performed and managed through this interface. Moving these functions out onto the Internet has provided increased accessibility and ease of use for customers and

[19] Computer Security Institute, "Frontline End-User Awareness Newsletter," 2001 (cited 15 January 2003); available at https://wow.mfi.com/csi/order/frontline.html

[20] SANS Institute, "Newsletters and Digests," 2002-2003 (cited 27 November 2002); available at http://www.sans.org/newsletters

[21] Association for National Computer Security Day, 2002 (cited 12 November 2002); available at http://www.computersecurityday.org

employees, and has dramatically reduced costs and increased efficiency in this area. It is GIAC's first strategic step in long-term plans to move additional business functions out into the Internet environment.

The background application and databases tied to the ERS interface contain vital customer information, and course registration, scheduling and delivery data critical to other functional areas of GIAC's business. Impact on the accessibility and/or integrity of this data would also seriously hamper operations in these areas.

These key assets enable GIAC to cost-effectively expand the reach of marketing campaigns, provide online course registration and scheduling services for customers, and support related planning and management operations. High reliability and accessibility of these assets must be assured to support these functions.

Malicious attackers could identify and exploit known vulnerabilities in GIAC's web server environment to gain entry, altering site content for their own purposes and/or causing a loss in availability of the site and its ERS interface. A secondary concern would be attackers exploiting known vulnerabilities in the database server behind the ERS interface. This could result in damaged or lost data, and/or data integrity issues. Database servers tied to Internet applications are often overlooked because they are viewed as back-end systems that are not as vulnerable as the web server exposed to the Internet. Critical databases can however, often be accessed through an insecure web server or web application.

Relevance

The Windows operating systems and Internet Information Services (IIS) software on GIAC's Internal Mail Server has not been kept up to date with the latest Service Pack and security patches. Likewise, the Windows operating systems and SQL Server software on GIAC's Database Servers has also not been kept current.

Keeping system patches and fixes is a critical security "best practice" that cannot be ignored, particularly in systems connected to the Internet. Proper preventive maintenance in this area enables the identification and elimination of problems before they enable failures or loss of accessibility, integrity and confidentiality to occur.

Multiple pieces of exploit code for recently announced vulnerabilities in Windows 2000 have been made public by security industry services. With the release of each Security Bulletin regarding these vulnerabilities, Microsoft has urged Windows administrators to patch their systems against these vulnerabilities.

The most recent and critical of these vulnerabilities in the Windows 2000 operating system involved IIS being used as the attack vector to exploit the flaw.

IIS users had no window of time to patch their systems because the flaw has already been exploited.[22] The attack involved sending a specially crafted request to an IIS 5.0 server with WebDAV running, which if successfully exploited, could allow attackers to run arbitrary code on the system. Initially, it effected systems running WebDAV on Internet Information Services (IIS) Web Server version 5.0, however it was subsequently found that other applications could also be used to exploit the flaw.

According to industry experts, most operating system exploits involve known software vulnerabilities. The Solar Sunrise Pentagon incident, Code Red and NIMDA worms, and SQL slammer virus are all examples where known vulnerabilities were used with widespread and devastating impact.[23] The speed and widespread impact of some of the more efficient worms, including Code Red and Nimda, was attributed to improper IIS server configurations.

Microsoft has issued multiple patches for SQL Server to fix more than ten recent security vulnerabilities. Even behind a firewall, attackers have found effective ways to get to background databases and SQL Server services.

The need to properly maintain database servers was exemplified by the unprecedented disruption of services recently caused by the SQL Slammer worm infection. According to industry reporting services, it spread so fast that it infected more than 90 percent of vulnerable computers within 10 minutes, and analysts estimated well over a billion dollars in lost productivity. Slammer's real cost however, was its immediate impact on customers. Airplanes were not taking off, emergency call center computers were effected, bank ATMs were not giving cash, people could not get a dial tone, access to the Internet was shut down and so on. Things were clearly not "business as usual" for those effected.

By not identifying system vulnerabilities and keeping these critical system components current, GIAC runs a higher risk of attackers using vulnerable systems and exploiting known vulnerabilities as vectors for attack.

Potential Impact and Consequences

Loss of accessibility of the Internet server would disrupt GIAC's ability to market their products and services. It would also adversely effect their ability to efficiently conduct critical business operations and deliver services related to course registration, scheduling and delivery.

---

[22] Edward Hurley, "New critical IIS buffer flaw exploited," in TechTarget Network [electronic newsgroup], (18 March 2003 [cited 21 March 2003]); available at http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci886661,00.html

[23] SANS Institute, "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts' Consensus," 2002-2003 (cited 27 December 2002); available at http://www.sans.org/top20

If breached, GIAC's web site could be the target of defacement, denial of service attacks or other malicious activity. GIAC servers could also be used as a launching point for attacks against other entities via the Internet. Such an attack could also jeopardize the accessibility and integrity of databases that contain confidential customer data and critical registration, scheduling and delivery information.

GIAC could suffer major losses in business opportunities and productivity, damage to or loss of network and/or information assets, and damage to reputation and customer/public trust.

There are also reasonable expectations that enterprises with IT assets that are linked to the Internet will ensure their systems are sufficiently secure, so that they cannot be used to harm another entity's assets. GIAC could be exposed to litigation based on a breach of duty, if it was proven that they failed to meet this obligation not patching systems exposed to the Internet, and their negligence resulted in damages to other parties.

Mitigation Strategies

The following risk mitigation steps are proposed:

- Update Internal Mail Server Windows 2000 operating system software, Internet Information Services (IIS) 5.0 software with the latest Service Packs and security patches.
- Update SQL Server 2000 software with the latest Service Packs and security patches.
- Inventory and assess vulnerabilities across these systems, particularly known critical Internet security vulnerabilities. The SANS/FBI Top Twenty list summarizes the most critical Internet security vulnerabilities and provides detailed information on the ten most commonly exploited vulnerable services in Windows, and the ten most commonly exploited vulnerable services in Unix.[24] Use analysis results to prioritize and alleviate vulnerabilities that pose the most risk. This approach will maximize security improvements and return on mitigation efforts.
- Develop and implement routine assessment and patch management policies and protocols to assure systems are kept current. Standard operating procedures should include steps to ensure hotfixes and patches are properly evaluated and tested. Having such procedures assures each update is appropriate for the environment, and determine if it needs to be done immediately, or can wait until the normal system maintenance cycle or the release of a cumulative patch or service pack.

[24] SANS Institute, "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts' Consensus," 2002-2003 (cited 27 December 2002); available at http://www.sans.org/top20

To increase efficiency and reduce the workload involved in identifying and manually applying patches to vulnerable systems, GIAC should explore and evaluate available products that could be used to automate vulnerability scanning and analysis, and assist or automate the patch management process. The tools selected for these purposes will depend on needs, resources, platforms and risk mitigation requirements. While no particular product recommendations are being made, evaluation might include:

- Microsoft "installers" to automate the process of patch installation, or Microsoft's free patch management program, System Update Server (SUS) to set up an update server on the network to download new updates automatically or at the direction of an administrator upon approval of each patch.
- Microsoft's free Baseline Security Analyzer (MBSA)[25] which performs local or remote scans of Windows systems.
- HFNetChkPro or the free version HfNetChkLt[26], which support automated scanning and analysis of most widely used platforms and products, along with patch installation management and patch application validation.
- Security scanning and auditing tools such as NGSSQuirrel[27] a security audit and management tool specifically for SQL Servers.
- Software patch vulnerability assessment and management solutions like UpdateExpert[28] which automatically scans networked systems for missing patches and downloads patches needed to remediate discovered weaknesses to a designated server. Patch Manager 2.0[29] is another such solution that can proactively identify and assess systems for known critical vulnerabilities and efficiently manage applying critical updates to areas of vulnerability across an environment.

It is not enough however, to put policies in place and procure scanning and update tools. GIAC must actively commit to putting the process and tools to work. Patching systems is not an option anymore – it must be done diligently, today, tomorrow, and every day thereafter.

Reviewing and ensuring application security and data validation checks are in place within the ERS application layer and related databases will further reduce the likelihood of data loss or integrity issues from such an incident.

[25] Microsoft Corporation, "Microsoft Baseline Security Analyzer," 2003 (cited 27 Feb 2003); available at http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/Security/tools/tools/MBSAHome.asp
[26] Shavlik Technologies, LLC, "Products" 1997-2003 (cited 27 February 2003); available at http://www.shavlik.com/pProducts.aspx
[27] Next Generation Security Software Ltd, "NGSSquirrel," 2002 (cited 27 February 2003); available at http://www.nextgenss.com/software/ngssquirrel.html
[28] St. Bernard Software, "UpdateEXPERT," 2001-2003 (cited 27 February 2003); available at http://www.stbernard.com/products/updateexpert/products_updateexpert.asp
[29] BigFix, Inc., "Patch Manager 2.0," 2002 (cited 27 February 2003); available at http://www.bigfix.com/website/about/releases/pr_0217032.html

GIAC should examine and consider database security best practices in this area, including but not limited to:

- Applying all vendor-supplied patches in controlled, timely manner.
- Implementing additional defense-in-depth strategies such as a properly configured internal firewall in front of critical database assets.
- Ensuring the database log-in has a strong password and keep databases insulated through tight controls on access. Apply the principle of "least privilege," to ensure individual access permissions are limited to data and services appropriate and required to perform their job duties.
- Ensuring auditing is turned on and audit logs are reviewed regularly.

3. Risk / Threat

The loss of availability of electronic communication (email) capabilities due to a hard disk failure presents a serious business risk for GIAC.

All functional departments within GIAC depend heavily on reliable access to email, shared contract and project management software and files. GIAC employees rely on email to efficiently and effectively communicate and electronically share information with partners, customers and remote users. Efficient internal communication and electronic exchange of information between functional departments is key to efficient operations.

Reliable electronic communications are critical to enable employees to effectively coordinate and manage multiple training projects. The availability of this asset must be assured to maintain efficient and effective communication, information sharing and productivity.

Relevance

GIAC's email services are supported on hardware that is at or beyond its normal end-of-life expectancy, is thus more susceptible to hard disk failures.

While even new equipment is susceptible to hard disk failures, the probability of disk failure is much higher when equipment ages beyond 2-3 years. It is also harder to obtain replacement parts and ensure maintenance services. Aside from planned replacement, there is not much more one can do to prevent hard disk failures when faced such circumstances. However, proper backup and recovery procedures can go a long way toward ensuring minimal disruption or loss of business functions should such an incident occur.

While the infrastructure exists to support it, GIAC does not have proper controls in place to ensure backup procedures for these resources are consistently performed in a routine and scheduled manner. Without proper backup

assurance, restoration of critical information assets and system resources cannot be ensured in the event of such a failure.

Ensuring regular scheduled backups of shared servers, files, applications and databases is an integral requirement of doing business in a networked environment. Servers are subject to mechanical failures; drives wear out or crash. Software and operating system failures can also cause file loss or damage. Desktop user or system administrators can inadvertently or maliciously delete important files or databases. Applications, files and data can become corrupted or destroyed by malicious programs. Communication failures, virus infections, application failures, natural or man-made disasters such as electrical outages, fires, water damage and weather related events can render damage to files, databases and/or the equipment they reside on and/or are accessed through.

The potential risk for GIAC is extremely high as GIAC's business operations rely heavily on access to email services and the ability to electronically share files and information. Routine and effective backup strategies are essential to ensure integrity and availability of these resources.

Potential Impact and Consequences

Loss of accessibility would seriously disrupt internal and external communications and workflow. GIAC would be forced to resort to verbal and paper communication processes, greatly reducing efficiency and productivity. Access to critical communications, and the ability to share information and work products in electronic format would be rendered impossible.

Critical business records and communications would be unavailable. The impact on GIAC's bottom line would eventually be seen in lost business opportunities, reduced productivity and profits. Extensive periods of loss of accessibility could effect their ability to deliver services and meet contractual obligations.

Mitigation Strategies

The following risk mitigation steps involving tape backups, data replication, standby hardware and contingency/disaster planning and equipment replacement considerations, will help ensure email capabilities are readily available:

- For the longer-term, develop a replacement plan for critical network infrastructure components; consider servers with built in real-time replication features.
- Develop and implement a backup and recovery plan, policies and procedures designed to ensure that the servers that support GIAC's email services are adequately backed up so that resident information and software is preserved and protected from loss or destruction. A

time-delayed tape backup capability will provide the best chance for salvaging data. Critical files and data can generally be restored as long as routine backups are regularly performed and recovery procedures are in place. System configuration backups are also a critical element. The key to prevent data loss and ensure efficient recovery is planning. Recovery procedures depend to a large extent, on proper assessment of what resources and information assets are considered critical to GIAC's business operations, and the supporting backup and restore procedures that are required to assure business can continue in the event of loss.

- Educate administrators and users on the importance of backups using examples that portray the impact on critical operations and routine tasks. Enlist management help in identifying applications files and data most critical to GIAC operations.
- Create a policy that makes backups mandatory where appropriate so it is not viewed as an optional activity. Make backup procedures consistent and easy, and automate wherever possible.
- Implement routine audit procedures to assure backup compliance.
- Implement a "Grandfather-Father-Son" backup scheme to ensure data accessibility and reliability. This strategy uses daily (son), weekly (father), and monthly (grandfather) backup sets[30] to assure availability of critical files and applications.
- Where appropriate, store copies of critical GIAC files and applications, and a copy of backup and recovery plans in a secure off-site location for recovery purposes. Retain a current copy on-site for immediate repairs caused by minor problems.
- Ensure those responsible have adequate and appropriate hardware and media to perform backup and maintain an adequate history. If this is not addressed, administrators may take a calculated risk regarding what needs to be backed up and critical data may be lost.
- Determine appropriate record retention periods and build them into the backup procedures.
- To keep downtime to a minimum, make standby and contingency arrangements for critical hardware, software and human resources required to effect rapid restore and recovery. Identify other organizations or service providers that could assist if needed.
- Review and test backup and recovery plans on a routine basis but no less than annually, using realistic case scenarios, to ensure they remain viable. Conduct "worst case scenario" drills to validate that plans and procedures will actually work. Revisit backup plans when significant changes to systems, applications or processes occur.
- Ensure management signs off on backup and recovery plans as meeting their needs.

[30] Dlttape.com, "The Three R's of Data Protection – Grandfather-Father-Son," 2002 (cited 1 February 2003); available at http://www.dlttape.com/ThreeRs/Reliability/Rotation/Grandfather.htm

- Ensure backups are maintained at the same standard of security that the original data is held to.
- Consider insurance coverage to cover the organization in the event of irreparable loss or damages.

SECTION 3

This section provides an evaluation of an existing policy intended to address one of the critical risks identified in Section 2 above. It seeks to identify the strengths and weaknesses of the sample policy, and presents a revised version of the policy tailored to suit GIAC's needs.

The Security Awareness Training policy example being evaluated was obtained from the New Hampshire and Vermont Strategic HIPAA Implementation Plan web site. The full policy text and the URL where it is published online are provided in *Appendix A*.

Evaluation of Existing Security Policy

The following evaluation is based strictly on the requirements of this practical and is not intended in any way to be a criticism of the policy or the authors of said policy. The intention is solely to analyze and evaluate the policy in accordance with the guidelines and framework conveyed in the SANS GISO course, and its applicability for GIAC, and then, to present a revised policy to address the gaps identified in the evaluation and fit GIAC's business model and requirements.

This policy topic was selected based on its relevance to GIAC's needs and addresses one of their three most critical areas of risk, and supports reducing risk in the other two. The author was also keenly interested in exploring this policy topic, as examples specifically designed to address the overarching need for security awareness training seem less prevalent, yet the author's company and many industries are mandated or driven by common sense and due diligence to provide such training.

General Evaluation: It is evident that the policy is intended to address the issue of security awareness training as it relates to computer and communication system users. The scope of the policy is not as clear as it should be regarding who and what is effected. Guidelines and best practices are presented that lend some understanding as to how compliance with the policy might be carried out, however it is unclear as to what procedures are most critical or what should be done at minimum to be considered as having complied with the policy. The policy fails to speak to who is responsible or what represents compliance.

Purpose: The purpose of this policy is not as clear as it should be. The purpose does not adequately describe why the policy is being established. It does not

speak to what issue or risks it is meant to address. It also includes the word "adequate", a vague adjective that can be interpreted differently from individual to individual and conveys a sense that the "minimum" will be acceptable. A clearer and stronger statement of purpose could be made by rewriting this section to indicate the purpose is to assure all individuals who have access to GIAC's information and computing environment receive security awareness training on a defined and scheduled basis, in compliance with GIAC's Security Policy and Security Awareness Training Policy.

Background: The policy does not contain an overview or any background to expand on the purpose or provide additional justification or support for the policy. This makes it difficult for the reader to put it into the appropriate context.

Scope: The scope of the policy is broken out into two sections that seem at first read to be relatively clear as to who and what systems are effected because the statements are all-inclusive (I.e., all means everyone). However, all users could be interpreted to mean only employees, or just end-users, thus not including vendors or technical staff who interface with the systems and/or have access to administer and support systems. It could be improved by combining the two sections into one more clearly written scope statement.

Policy Statement: The policy statement does not do a sufficient job of clearly stating what is to be done, or providing any guiding principles, goals, objectives or expected outcomes. The title and purpose seem misaligned when compared with the policy statements. Clearly stating what will be implemented and how it will be carried out would convey a more understandable message of intent. The policy also does not speak to how effectiveness and compliance will be evaluated and what frequency or criteria will be followed. It is vague insofar as how it relates to the scope, and the statement regarding users who violate the policy is out of place in this section.

Responsibility: The policy does not provide any information as to who is responsible for the policy, ensuring it is successfully implemented as intended or for carrying out policy directives. It also does not provide any information as to who can draft, review, approve or modify the policy. This conveys a sense that the policy may not be considered sufficiently important enough to maintain or enforce. A policy that is not enforced is ineffectual and simply ends up being a "paper tiger" not to be taken seriously.

Action: The policy does not contain any details as to what specific actions are required or when they should be accomplished. There is no direction as to what steps are required to actually carry out the policy and who will perform them. The addition of compliance dates for set tasks, evaluation or assessment actions, a reference to planned quarterly reviews and/or revision dates, would help establish expectations in these areas.

Revised Security Policy

1.0 Overview and Background

GIAC's information assets and technical infrastructure are among our most valuable assets, and are critical to business activities. The availability and integrity of information is key to our ability to carry our mission. Assuring the security of information assets, systems and technologies that support our everyday operations is the responsibility of every employee. Each authorized user of GIAC information has an obligation to follow good security practices to preserve and protect GIAC's information assets and system resources in accordance with our Security Policies. Security awareness is the foundation of sound security practices.

GIAC supports training in all functions required for employees to perform their job duties and contribute to the overall success of the organization. Security awareness training increases knowledge of security issues, enables employees and system users to understand what they are expected to do, and enhances their ability to recognize and prevent internal and external threats and risks to GIAC's information assets. GIAC's Security Awareness Training Policy addresses these issues through a structured training program designed to enhance security awareness and improve GIAC's overall security practices.

2.0 Purpose:

The purpose of this policy is assure that all individuals who have access to GIAC's information and computing environment receive security awareness training on an annual basis, in compliance with GIAC's Security Policy and Security Awareness Training Policy.

3.0 Related Documents:

- GIAC Security Policy.

4.0 Scope:

The scope of this policy includes all personnel, including administrators, managers and end users, temporary staff, interns, consultants, contractors and any other external entities that use, interact with or perform administrative services on GIAC's computer systems and/or data.

5.0 Policy Statement:

As a condition of employment, all GIAC personnel must attend an initial Security Awareness Training Program and sign a GIAC Confidentiality Agreement upon hiring. Personnel must also attend annual Security Awareness Training Refresher Sessions as appropriate for their role and responsibilities, and must

update and sign the Confidentiality Agreement on annual basis, concurrent with their performance evaluation.

Temporary staff, interns, consultants, contractors and other external entities performing services that involve access to, use, interaction or administrative of GIAC's computer systems and/or data must attend GIAC Security Awareness Training and sign the Confidentiality Agreement and the Non-Disclosure form associated with their individual contract or scope of work agreement.

These requirements must be complied with before any authorized access to systems or data will be granted. To ensure consistency, there are no exclusions to this policy, unless expressly authorized by the CEO.

6.0 Responsibility:

- The Information Security Officer is responsible for issuing this policy and responding to inquiries regarding it.
- Human Resources is responsible for scheduling and coordinating training, assuring individuals attend, retaining signed Confidentiality Agreements and Non-Disclosure Forms on file and making them available for review.
- Security Services is responsible for assuring that individuals are not granted access to systems or data unless the requirements in this policy have been met.
- The Information Security Officer is responsible for drafting any proposed revisions and submitting them to GIAC Management for review. Proposed modifications regarding this policy should be submitted to the Information Security Officer in writing.
- The Information Security Officer is responsible for assessing this policy has been successfully implemented and reporting compliance and training effectiveness outcomes to the CEO on a quarterly schedule.

7.0 Actions:

The following actions will be taken to facilitate implementation and support of this policy. These actions will convey clear and consistent expectations regarding this policy, GIAC's stance on information security, and the importance of protecting GIAC assets.

- The Training Division and Information Security Officer will jointly develop and maintain GIAC's Security Awareness Training Programs.
- The Training Division will carry out the delivery and evaluation of GIAC Security Awareness Training Programs.
- The Information Security Officer will formally issue the policy with a cover memorandum reflecting the purpose, key concepts and impact, and publish it on GIAC's intranet web site to make it easily accessible. The Information Security Officer will also brief Sr. Management on the policy.

- Human Resources will assure all individuals have attended the required Security Awareness Training Program by no later than September 1, 2003, and report progress in the month-end management report.
- GIAC Management will ensure that all individuals that fall within their areas of responsibility comply with this policy.
- Supervisors will review GIAC's security policies with the individual as part of each employee's annual evaluation review, and obtain their signature on the appropriate Confidentiality Agreement and/or Non-Disclosure Form.
- The Information Security Officer will, in cooperation with Human Resources, integrate the policy's concepts into the GIAC's new hire orientation materials by no later than September 1, 2003.
- The Information Security Officer will conduct random reviews on a semi-annual basis, to verify policy compliance.
- All GIAC security policies and revisions will be approved and signed by the CEO to ensure executive management support.

8.0 Compliance and Enforcement

Any GIAC employee found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Non-employees (temporary staff, interns, consultants, contractors and other external entities performing services) found in violation of this policy may be subject to action or dismissal based on the terms or their contractual relationship with GIAC.

9.0 Revision History

Version: 1.0 – Initial Release
Revision Date: February 1, 2003
Effective Date: February 1, 2003
Issued by: Deborah Snyder, Information Security Officer, GIAC

Signed: _____ Date: _____
CEO, GIAC

SECTION 4

This section provides operational procedures that will be used to implement the policy developed in Section 3 above. While a series of multiple procedures would be involved in implementing the above policy, this section is only intended to detail a single procedure. The procedure addressed is performed by Security Services in meeting their responsibility to assure that individuals are not granted access to systems or data unless the requirements within this policy have been met.

Security Policy Procedure

The following outlines one of the step-by-step procedures that will be used to implement and enforce GIAC's Security Awareness Training Policy. The

following procedure only addresses the process of submitting, reviewing, processing and approving requests for access. Implementation actions will be carried out by those described as being responsible within the Security Awareness Training Policy.

Procedure Steps:

1) All persons requesting or requiring access to GIAC systems and data must submit a GIAC Access Request Form, completed and signed by their supervisor/manager, to Security Services.
2) Security Services will acknowledge, review and respond to all Access Requests received within five (5) business days of receipt to determine if the individual should be granted access.
3) Security Services will confirm with Human Resources that the requesting individual has attended the required Security Awareness Training and signed the appropriate Confidentiality Agreement and/or Non-Disclosure Forms.
4) If access is approved, Security Services will establish the appropriate user access account following GIAC's User Access Account Management Procedures and Role-Based Access Guidelines. Permissions will be granted based on the principle of minimum access required to perform assigned duties.
5) Disagreements in permission levels will be resolved through discussion and justification of access needs between the IT Director and individual's Supervisor and Division Director.
6) Security Services will notify the requesting individual and their supervisor/manager of their determination, and if approved, provide the access account information to the requesting individual.
7) Security Services will review all access accounts against personnel records on a quarterly basis to identify and resolve any variances.
8) Accounts that are inactive over thirty (30) days will be administratively closed by Security Services.

Appendix A -- Sample Security Policy

The following Security Awareness Training Policy example was obtained from the New Hampshire and Vermont Strategic HIPAA Implementation Plan web site, where it is published as a sample policy to provide guidance to their member organizations.
HTTP://WWW.NHVSHIP.ORG/DOWNLOAD/SECURITYAWARENESSTRAININGPOLICY.HTM.

Security Awareness Training Policy
DRAFT

Purpose
Ensure that an adequate information security awareness training program is developed and administered by the <ABC COMPANY>.

Policy
A program to provide information security awareness training will be developed, and administered by the <ABC COMPANY>. System users who violate this policy will be subject to disciplinary action.

Who is affected:
All authorized system users who have access to electronic information containing personally identifiable healthcare information.

Affected Systems:
This policy applies to all computer and communication systems utilized by the <ABC COMPANY>, and its subsidiaries.

Guidelines/Best Practice

- Orientation program exists for all first-time employees.
- Continuing education program is administered for all system users including annual formal class sessions, and periodic reminders, alerts, and distribution of other written materials.
- Initial and continuing education programs are evaluated for learner achievement, relevancy of content, and effectiveness of instructional delivery.
- Security user manual is distributed and policies explained to all employees.
- All system users are instructed in the proper use of information systems according to their job tasks.
- Each system user is required to sign a confidentiality agreement and a statement that they have read, understand, and agree to comply with the security policies and procedures of <ABC COMPANY>.

- Confidentiality agreements are updated and signed on an annual basis.

Effective Date:

Approved:

_____	_____
President	Chief of Staff
_____	_____
VP/Chief Financial Officer	VP/Chief of Patient Care & Operations

Original:

Dates Reviewed:

Dates Revised:

REFERENCES

Association for National Computer Security Day. 2002. URL: http://www.computersecurityday.org (12 November 2002).

BigFix, Inc. "Patch Manager 2.0." 2002. URL: http://www.bigfix.com/website/about/releases/pr_0217032.html (27 February 2003).

Bitpipe, Inc. "Return to Business Value - Gaining ROI from Enterprise System Management." 1 January 2002. URL: http://www.bitpipe.com/data/detail?id=1036096051_748&type=RES&src=FEATURE_RESTRM&x=1888050311 (31 January 2003).

Cisco Systems, Inc. "SAFE Blueprint for Small, Midsize and Remote-User Networks." 2001. URL: http://www.cisco.com/en/US/netsol/ns110/ns129/ns131/ns128/networking_solutions_implementation_white_paper09186a008009c8a0.shtml (5 January 2003).

Cisco Systems, Inc. "Cisco 1710 Series Access Routers, Technical Details." 2003. URL: http://www.cisco.com/en/US/products/hw/routers/ps221/prod_technical_details.html (17 February 2003).

Cisco Systems, Inc. "Cicso PIX 500 Series Firewalls." 2003. URL: http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/prod_technical_details.html (15 February 2003).

Cisco Systems Inc. "Cisco Catalyst 3550 Series Switches." 2003. URL: http://www.cisco.com/en/US/products/hw/switches/ps646/products_data_sheet09186a00800913d7.html (19 February 2003).

Cisco Systems Inc. "Cisco Catalyst 2950 Series Switches." 1992-2003. URL: http://www.cisco.com/en/US/products/hw/switches/ps628/prod_technical_details.html (17 February 2003).

Cisco Systems Inc. "Catalyst 2900 Configuration Guide." 1992-2003. URL: http://www.cisco.com/univercd/cc/td/doc/product/lan/cat2900/index.htm (17 February 2003).

Computer Security Institute. "2002 Computer Crime and Security Survey." 7 April 2002. URL: http://www.gocsi.com/press/20020407.html (22 November 2002).

Computer Security Institute. "*FrontLine* End-User Awareness Newsletter." URL: https://wow.mfi.com/csi/order/frontline.html (15 January 2003).

Cooper, Russ. "Hardening Windows." Information Security Magazine. January 2003 (2003): 44.

Crume, Jeff. Inside Internet Security – What Hackers Don't Want You to Know. London: Pearson Education Limited, 2000.

Davis, Jeff. "Download our posters to raise awareness about IS security." 29 October 2002. URL: http://www.techrepublic.com/article.jhtml?id=r00320021029jed01.htm&fromtm=e101-3 (17 January 2003).

Dlttape.com "The Three R's of Data Protection – Grandfather-Father-Son." 2002. URL: http://www.dlttape.com/ThreeRs/Reliability/Rotation/Grandfather.htm (1 February 2003).

Element K Press. "Courseware." 1997-2003. URL: http://elementkcourseware.com/basics/home.jsp (31 January 2003).

Fisher, Dennis. "New Dangers Exposed in the Wake of Slammer." eWeek Magazine. February 2003 (2003):1, 12.

Hurley, Edward. "Testing Password Strength Gives Policy Some Bite." TechTarget Network. 29 October 2002. URL: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci858747,00.html (17 January 2003).

Hurley, Edward. "New critical IIS buffer flaw exploited." TechTarget Network, 18 March 2003. URL: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci886661,00.html (21 March 2003).

McCarthy, Mary Pat. Campbell, Stuart. Security Transformation, Digital Defense Strategies to Protect Your Company's Reputation and Market Share. New York: McGraw-Hill, 2001.

Messmer, Ellen. "Next 'Slammer Could Be Worse." Network World Magazine. February 2003 (2003):1, 57.

Microsoft Corporation. "Microsoft Baseline Security Analyzer." 2003. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/Security/tools/tools/MBSAHome.asp (27 February 2003).

Shavlik Technologies, LLC. "Products." 1997-2003. URL: http://www.shavlik.com/pProducts.aspx (27 February 2003).

National Institute of Standards and Technology. "NIST Systems Administration Guidance for Windows 2000 Professional - Special Publication 800-43." 2002. URL: http://www.csrc.nist.gov/itsec/NIST_W2K (20 December 2002).

National Institute of Standards and Technology. “Risk Management Guide for Information Technology Systems – Special Publication 800-30.” October 2002. URL: http://www-08.nist.gov/publications/nistpubs/800-30/sp800-30.pdf (2 December 2002)

New Hampshire and Vermont Strategic HIPAA Implementation Plan “Security Awareness Training Policy.” URL: HTTP://WWW.NHVSHIP.ORG/DOWNLOAD/SECURITYAWARENESSTRAININGPOLICY.HTM. (31 January 2003)

Next Generation Security Software Ltd. “NGSSquirrel.” 2002. URL: http://www.nextgenss.com/software/ngssquirrel.html (27 February 2003).

Ozier, Will. Risk Assessment and Management, Data Security Management. Boca Raton: CRS Press LLC, 1995.

Peltier, Thomas R. Information Security Policies, Procedures and Standards. Boca Raton: CRC Press LLC, 2002.

Peltier, Thomas R. Information Security Risk Analysis. Boca Raton: CRC Press LLC, 2002.

Robinson, Jarvis. “Internal Threat – Risks and Countermeasures.” 15 November 2001. URL: http://www.sans.org/rr/threats/internal.php (22 November 2002).

SANS Institute, The. GIAC Information Security Officer Training. Track 9.

SANS Institute, The. “Newsletters and Digests.” 2002-2003. URL: http://www.sans.org/newsletters (27 November 2002).

SANS Institute, The. “The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts’ Consensus.” 2002-2003. URL: http://www.sans.org/top20 (27 December 2002).

Shavlik Technologies, LLC. “Products.” 1997-2003. URL: http://www.shavlik.com/pProducts.aspx (27 February 2003).

St. Bernard Software. “UpdateEXPERT.” 2001-2003. URL: http://www.stbernard.com/products/updateexpert/products_updateexpert.asp (27 February 2003).

Tipton, Harold F. Krause, Micki. Information Security Management Handbook, 4th Edition. Boca Raton: CRC Press LLC, 2000. 258.

Woods, Charles Cresson. Information Security Policies Made Easy. Houston: Pentasafe Technologies, Inc., May 2001.