Global Information Assurance Certification Paper

GIAC Information Security Officer

Practical Assignment

Version 1.2

Protecting Information Assets in the Electronic Age: Risky e-Business in Pharmaceuticals

Janis A. Orsino, CISSP

April 15, 2003

GIAC Enterprises Introduction and Business Operations Overview....5
IT Infrastructure....5
Business Operations....9
Critical Risk Areas....14
Trade Secret Misappropriation....14
Threat or Risk Overview....14
Threat Significance to GIAC Enterprises....15
Feasible Consequences and Likelihood of Vulnerability Exploit....16
Steps to Mitigate the Risk....19
Potential Civil or Criminal Liability....20
Threat or Risk Overview....20
Threat Significance to GIAC Enterprises....21
Feasible Consequences and Likelihood of Vulnerability Exploit....21
Steps to Mitigate the Risk....23
Compromise of System / Data Integrity....24
Threat or Risk Overview....24
Threat Significance to GIAC Enterprises....24
Feasible Consequences and Likelihood of Vulnerability Exploit....24
Steps to Mitigate the Risk....26
Evaluate and Revise Security Policy....27
Evaluate Model Information Sensitivity Policy....28
GIAC Enterprises Information Sensitivity Policy (Revised)....30
Develop Security Procedures....30
Procedures for Information Sensitivity Policy Compliance Review....30
References....36
Appendix A: Model Information Sensitivity Policy....39
Appendix B: GIAC Information Sensitivity and Protection Policy (Revised)....46

Leave this page blank

Abstract

Information systems innovations and electronic data interchange (EDI) have revolutionized pharmaceutical research and development (R&D) efforts, and have broken from traditional individualistic research approaches and knowledge silos, by enabling the capture, categorization, and sharing of knowledge. With R&D knowledge opened to teams of scientists, and given the ability to conduct and manage clinical trials globally over multiple sites, pharmaceutical companies reduce development time and cost, increase innovation—and increase production of breakthrough treatments--ultimately increasing product revenue and competitiveness within the marketplace. Information systems have evolved from being important to being critical in the performance of these missions. However, even as the industry's dependence on information technologies has grown, so too have the vulnerabilities of these technologies and the range of threats inherent in them. In addition to creating a trusted environment for corporate trade secrets and protecting intellectual property valuations, pharmaceutical businesses have regulatory oversight. The Health Insurance Portability and Accountability Act (HIPAA), for example, was enacted to focus on an individual's personal health information. Thus, information systems innovation combined with increased accountability has created greater business challenges and security risks within the pharmaceutical industry.

This paper addresses aspects of an information security program within a large pharmaceutical company, defining its three critical risks areas, threats, vulnerabilities, and identifying safeguards, countermeasures and actions to mitigate those risks. As part of an effort to assess the adequacy of existing countermeasures relative to the most critical risk area, one issue-specific policy is evaluated. Upon evaluation, and in consideration of the risk assessment, the recommendations for new policy and procedure developments are provided to further safeguard against threats.

GIAC Enterprises Introduction and Business Operations Overview

GIAC Enterprises ("GIAC") is a multi-national pharmaceutical company dedicated to the discovery, development and manufacturing of novel target-based treatments focused primarily in three Therapeutic Areas: Cancer Biology, Neurology, and Immunological Disorders. Its global headquarters are based in Boston, Massachusetts, with research laboratories, manufacturing facilities, and regional sales offices in seven global locations including Sydney, Geneva, Tokyo, Frankfurt, and Milan.

IT Infrastructure

GIAC's IT infrastructure employs state-of-the-art technology to (1) support its business model; (2) ensure integrity of the core GIAC database in a 24 x 7, high availability operational environment; and (3) meet the global requirements addressed later in this document. GIAC has about 3500 users using the network at the Boston headquarters office (primary site) and at nine remote locations (secondary sites). In addition, about 360 users telecommute. Figure 1 depicts the basic components of GIAC's infrastructure as it is further explained in this section.

GIAC's infrastructure consists of heterogeneous operating systems and applications from multiple vendors. These systems are tightly integrated with state-of-the-art Cisco network security products to mitigate the technological risk associated with managing GIAC connections and geographically dispersed resources. The network security design and implementation are predicated upon several GIAC security policies and procedures, including the Authentication Policy, Access Policy, and IT System and Network Maintenance Policy.

GIAC employs a dual-homed hosting environment peered to two tier-1 Internet Service Providers (ISP), providing dedicated DS-3 (Digital Signal Level 3) (44.736 Mb/S T3 Interface) Internet pipes. Two Cisco 7206 routers configured with Enterprise IOS 12.3, enable connectivity between the GIAC network and ISPs. The two diversified Autonomous Systems (AS) running BGP4 (Border Gateway Protocol) provide multiple ingress and egress routes, ensuring continuous availability. The 7206 routers provide inbound IP filtering. BGP allows for MD5 hash peer authentication and route filtering based upon access control lists, both features providing added measures of security.

At the core are two Cisco Catalyst 6513 switches with dual Supervisor Engines (v. III) and redundant 1600-watt power supplies. Each Supervisor Engine includes a Multi-layer Switch Feature Card 2 (MSFC2) for Layer 3 switching. The 6513 switches are running Enterprise IOS v7.3, and the MSFC2s are running Enterprise IOS v12.1 (2). Each Supervisor Engine also includes two Gigabit Ethernet ports. There are four 6416 blades, each of which contains 16 Gigabit Ethernet ports. All of the Gigabit Ethernet ports require Gigabit Interface Converter (GBIC) modules for connectivity. The switches interconnect through

802.1q trunking over Gigabit fiber. The 6513 switches provide a port security mechanism to restrict Machine Address Code (MAC) addresses that can connect via a particular port of the switch, which is particularly useful in the face of MAC address flooding attacks.

The GIAC infrastructure consists of five Virtual LANs (VLAN): The "Public IP Network" (VLAN 10), the "Private DMZ Network" (VLAN 20), the "Private Production Network" (VLAN 30), the "Management Network" (VLAN 40), and the "Private GIAC Corporate Network" (VLAN 50). The 6513 switches running VTP2 are configured to be the root bridge on all VLANs. The VLANs are segmented with stateful Cisco PIX 535 Firewalls running PIX IOS v. 6.3(1). The PIX firewalls are configured with sub-interfaces to allow for scalability as well as isolation of certain networks.

Site-to-site VPN connectivity is established through a 3DES IPSec configuration on stateful Cisco PIX 535 Firewalls running PIX IOS v. 6.3(1). These firewalls, residing between the public and private DMZ, also provides stateful packet filtering, tracking each connection traversing all interfaces of the firewall. A redundant, hot standby unit is deployed as a fail-over measure to maintain concurrent connections through automatic stateful synchronization. Behind the PIX (DMZ)[*] 535 Firewalls, are two Cisco IDSMs (Intrusion Detection System Module) with up to date attack signatures. These sensors detect and block malicious packets designed for circumventing the firewall filtering rules. They protect against attacks launched internally as well as externally, (e.g. hijacking GIAC's resources to launch an attack on another entity).

In GIAC's primary site DMZ configuration, the PIX (DMZ) Firewall isolates the Web, DNS and Sendmail servers from the Public IP network, and further isolates database, mail and application servers within the private production network. Two Web servers operate on the NSA's distribution of Security-Enhanced Red Hat Linux with Apache Web Server. The third operates on Microsoft IIS version 5.0 Web server. All unnecessary services are disabled and binaries removed, with exception of http (TCP port 80) and https (TCP port 443), DNS update (TCP port 53), DNS lookup (UDP port 53), and SMTP (TCP port 25). The PIX (DMZ) Firewalls also perform NAT on each server within the DMZ, reducing the risk of IP Spoofing, SMURF, WinNuke, and most common Internet attacks.

The primary and secondary sites employ two-zone firewall configurations (Cisco PIX 535 Firewalls) with a centralized DMZ between the two zones. This design prevents the servers within the DMZ from direct access to the Internet through Network Address Translation (NAT) and stateful packet inspection. The PIX 535 includes with its stateful high-availability capabilities, integrated hardware acceleration for VPN, providing up to 95 Mbps of 3DES VPN and support for 2,000 IPsec tunnels.[1]

---

[*] To eliminate confusion for the multiple PIX 535 Firewalls, each will be referenced according to where they reside on the network: PIX (DMZ), PIX ((PROD) for production network), and PIX (LAN).

[1] "Cisco PIX 500 Series Firewalls". *Cisco, Inc. Home Page*. 2002. 3 Mar. 2003. <http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/>

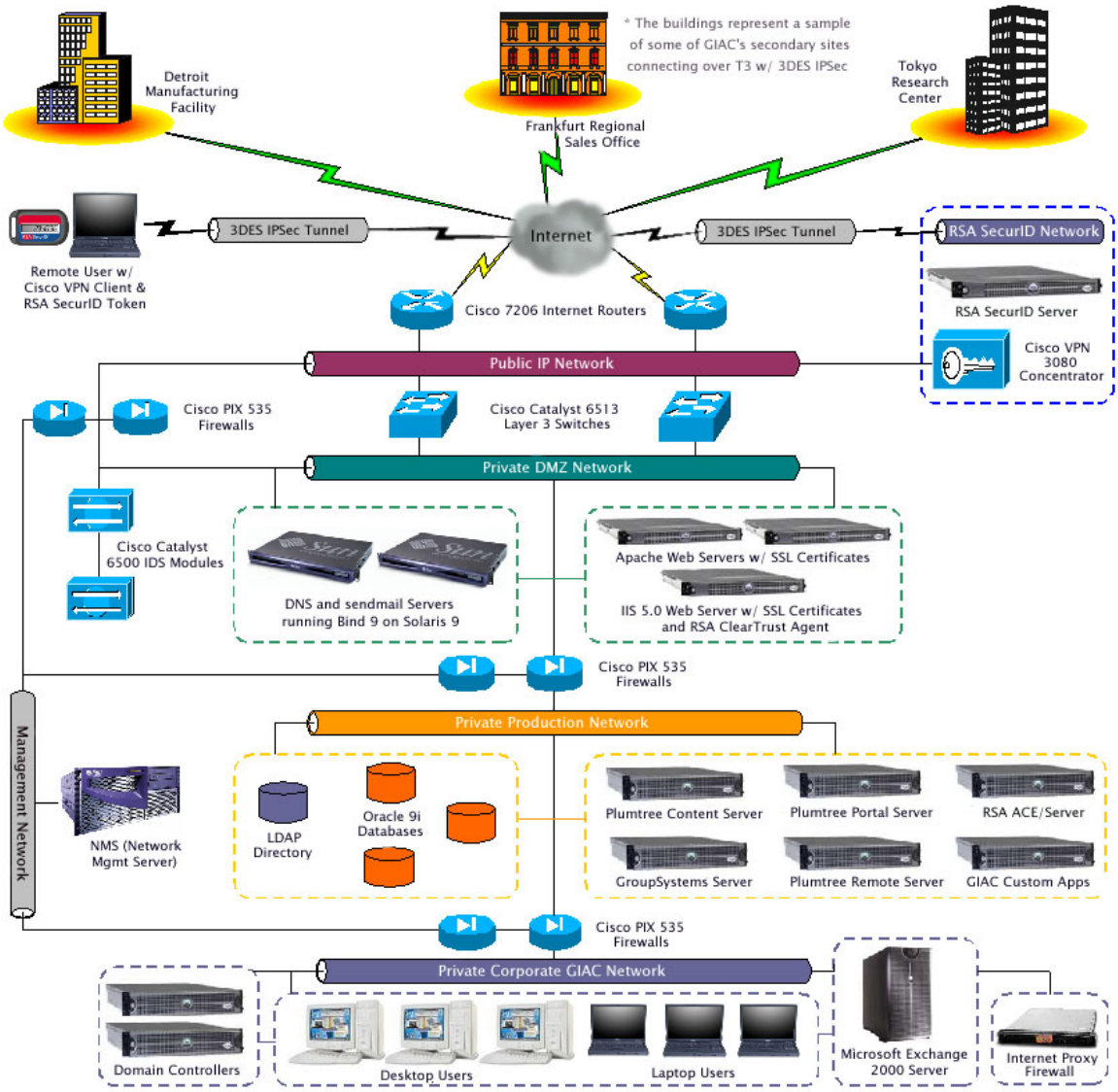

Figure 1: Physical Diagram of GIAC IT Infrastructure

Segmenting the database and application servers residing within the private production network from the DMZ is a second firewall zone - Cisco PIX 535 Firewall or "PIX (PROD)". With no direct connection to the databases the Web servers have to traverse a firewall to request content from the database. This design ensures that an end user out on the Internet cannot send a direct request to the database.

The VPN 3080 Concentrator is deployed in parallel with the firewall on the GIAC DMZ (Demilitarized Zone), and connected through the public Fast Ethernet port, so that the IPSec traffic passing between remote users and the concentrator is encrypted. The VPN 3080 is networked to the SecurID server through the "private" LAN interface. Any intermediate network devices (e.g. routers) are transparent to the VPN 3080.

GIAC's Cisco-based remote-access client Virtual Private Network (VPN)

implementation employs a strong authentication solution requiring only one infrastructure login. When a user connects to the Cisco VPN 3080 concentrator, the user is authenticated based upon a VPN group and one-time password generated by a SecurID token. Cisco VPN 3080 series enables both remote access and site-to-site VPN services using the IPSec protocol. This one operation authenticates the user to Microsoft Windows 2000 Active Directory, which enables remote access for multiple applications, and RSA ClearTrust Web software, which provides centralized management of user privileges. End users can connect remotely from laptops issued and certified by GIAC ITMD staff.

The GroupSystems application server provides an additional layer of authentication with a user ID and password issued by the GroupSystems application administrator. Access controls are role-based, based upon the users' need to create, modify, or participate in GroupSystems sessions. Users gain access to GroupSystems applications through client software installed on their laptops or workstations. Users must first be authenticated to the domain prior to attempting GroupSystems logon.

GIAC employs a proactive method for managing OS patches, updates and hotfixes across all servers and workstations on the network. St. Bernard Software's UpdateEXPERT is used to verify base configuration and automate the remediation process by determining the complexities, possible interdependencies and conflicts of potential updates, and deploying the necessary patches, hotfixes and service packs to servers and workstations on the network. A conformance report verifies policy adherence by reporting how the inventory matches up against required updates. Policy management is enforced by defining the policy (with required updates) and managing by exception those machines that are missing these required updates.

If UpdateEXPERT encounters questionable issues associated with installing a patch, the system administrator is alerted to manually evaluate it; determine whether it is applicable to the GIAC's servers and safe to install; and, if so, install it. In this event, updates are installed in an isolated test environment and a previously developed regression test suite is executed to compare current performance with past performance and verify that the patch does not conflict with installed software. After making any changes in a server's configuration or its information content, the administrator creates new integrity-checking baseline information for that server. Tripwire for Servers software is used to identify the changes made to files and directories. By creating another baseline and subsequently monitoring these changes, the administrator, over time, can identify unexpected changes that require further investigation. This process minimizes data integrity risks.

GIAC's data storage and backup solution incorporates Fibre Channel based connectivity between servers, databases, and storage devices for increased security, speed and efficiency in its backup process. All servers on the GIAC network are interconnected through Brocade fabric switch from EMC to a pair of Clarion EMC FC4700 Network-attached Storage (NAS) (not to be confused with Storage Area Network (SAN)) devices. The servers are backed up to an out of ban ADIC Scaler 1000 library. Each server is equipped with various

VERITAS backup software versions dependent upon the server operating system (see below).

Server Type	*Backup Software*
Win 2000 Servers	VERITAS Backup Exec 9.0 Suite
Linux Web Servers	VERITAS Software Enterprise Storage Management Solution for Linux-based Dell Server Platforms.
Oracle DB on Solaris 9	VERITAS Database Edition/Advanced Cluster for Oracle 9i
Win 2000 Exchange Server	VERITAS NetBackup 4.5 for Exchange
Sun Servers	VERITAS Volume Manager

The aggregate of hardware resources within the domain consist of Dell Dimension 4100, 1 GHz PIII, Win2K desktop workstations; Dell Latitude C640, 2GHz P4, Win2K laptops; HP LaserJet 4000TN and HP Color LaserJet 8550 printers; and Dell PowerEdge 2650 servers for the domain controllers. The mail server, Exchange Server 2000 Enterprise Edition, runs on the Dell PowerEdge 4600 configured with dual 2.0 GHz Intel Xeon processors, with 4 GB of DDR memory, and two-way direct-attached SCSI storage.

The Exchange e-mail server and domain controllers are configured with Windows 2000 Advanced Server and QLogic Fibre Channel Host Bus Adapters (HBA) providing secure connection to the switch fabric for back-up and recovery. Using the Fibre Channel HBA prevents data sniffing across the switch fabric. The domain controllers run the standard suite of file and print services for the end users in the domain.

The standard desktop configuration consists of Microsoft Windows 2000 Office Professional Suite, Internet Explorer, and custom applications. GroupSystems users require the GroupSystems client software. In addition to the standard configuration, laptops include the Cisco VPN client for Windows 2000. Additional applications may be installed based upon need, determined and approved by the employee's division director. Users are restricted from installing unapproved software by limiting user account permissions through Windows 2000 administration.

Business Operations

GIAC's primary business objective is to rapidly move novel, proprietary, small-molecule pharmaceuticals through pre-clinical development and into clinical trials. GIAC's strategic direction to develop breakthrough treatments, however, remains broad and scientifically entrepreneurial. Secondary to research and development (R&D) strategic business operations is manufacturing.

To support these key business operations, GIAC employs two levels of internal Technical Services groups that perform distinct roles. The Information and Technology Management Division ("ITMD"), located at the headquarters

office, primarily manages the final scale-up and the proliferation of processes to the various GIAC sites. Basically, ITMD has oversight control for technology development. The R&D Technical Services ("R&DTS") group develops technology processes for scientific research efforts, and is co-located with the largest research laboratory to observe processes and facilitating information sharing. R&DTS plays a key role in improving research effectiveness, enabling increased innovation, and facilitates knowledge sharing among project teams. The corporate Manufacturing Technical Services ("MTS") group develops the technology processes for new products, and is co-located with the largest manufacturing site. MTS "plays a key role in ensuring that safe and efficacious products reach the market by the most cost-effective methods".[2] With ITMD representatives at each site ensuring lows levels of autonomy among field offices, infrastructure and technical support issues remain relatively consistent.

For executive management, IT considerations are significant given the multitude of statutory, regulatory and standards compliance issues imposed by both by national and global sources. Due to concerns about internal costs, coupled with an increased focus from regulatory authorities on data handling, computer system validation, and manufacturing review processes, GIAC management has and will continue to rely upon vendors and consultants to meet compliance standards. Key issues to consider are those relating to the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA); the U.S. Food and Drug (FDA) Administration's Code 21 of Federal Regulations, Part 11, (21 CFR Part §11), particularly concerning electronic records and electronic signatures; and "the Codified Good Manufacturing Practice (CGMP), Regulations, Parts 210 and 211", particularly as these relate to manufacturing and product quality.[3] CGMP requires that domestic and foreign manufacturers have a quality system for the design, manufacture, packaging, labeling, storage, and delivery of finished medical pharmaceutical products intended for commercial distribution in the United States. The FDA monitors problem data and inspects the operations and records of pharmaceutical manufacturers to determine compliance with the CGMP requirements, and the agency may audit any manufacturing plant anywhere in the world.[4]

To achieve the right balance between end-user convenience and security needed to meet CGMP and HIPAA compliance goals, GIAC created a portal, the GEIS ("GIAC Enterprises Information System"), with security provided by two third-party solutions: RSA SecurID two-factor authentication software and RSA ClearTrust Web access management software. SecurID requires that the remote user identify themselves in two ways – by supplying a one-time code produced by a physical token and the user's PIN code. The combination of two-factor

---

[2] *Best Practices, LLC.* "Sample Report Summary: Pharma Technical Services: Structuring for Manufacturing Process Ownership." 12 Jan. 2003. <http://www.benchmarkingreports.com/businessoperations /op84_technical_services.asp>

[3] *U.S. Food and Drug Administration (FDA) Home Page.* "Current Good Manufacturing Practice (CGMP) Regulations: Division of Manufacturing and Product Quality (HFD-320)." 9 Jan. 2003. Center for Drug Evaluation and Research. 13 Jan 2003. <http://www.fda.gov/cder/dmpq/>

[4] Perseid Software Limited. "Creating a Global IT Infrastructure for Clinical Trials". Oct. 2001. 17 Jan 2003 <http://www.emc.com/vertical/pdfs/life_sciences/EMC_clinical_trials.pdf>

authentication and role-based privilege management should position GIAC to exceed some of the key security and privacy guidelines under HIPAA.

With a liberal portal budget, the CIO chose to emphasize localized content control, turning to a contractor to deploy Plumtree Software's Corporate Portal and content-management technology with an Oracle back end. Plumtree Corporate Portal forms the core of the GEIS, and integrates with a range of GIAC business applications and Internet services, such as the U.S. Patent and Trademark Office (USPTO) Trademark Electronic Application System, reference works such as the Merck Manual, and the on-line Physician's Desk Reference.[5]

GEIS streamlines business processes across the entire company, benefiting personnel regardless of job function. Some examples of its features and utility include:

- Facilitates sharing of key data by all researchers and research entities--not just the primary researcher and prime research organizations.
- Manages the collecting and transmitting of patient profile information to the research liaison.
- Enables a company-wide secure solution for developing, maintaining and executing multi-country, multi-site clinical trials.
- Ability for R&D project teams to access, organize and reuse information that is key to R&D innovation.
- Provides a directory to healthcare publications, patent services, R&D, and reference works.
- Facilitates the flow of information among researchers and marketing personnel during all aspects of discovery, testing, market introduction and after-market verification/validation of efficacy.
- Improves analytical processes that result from having integrated clinical, financial and administrative data in a single repository during clinical trials.
- Stores all key documents involved in the clinical trials process.[6]

The largest GEIS component is the Plumtree Content Server module. This serves as the central document repository, managing the volumes of critical data produced from R&D, pre-clinical and clinical trial data, patient data, side-effect data, compound libraries, and all documentation required to support CGMP standards. While GEIS is not deemed a "mission critical" resource, the information resources that reside within it, are. As such, access and authentication are tightly controlled through an integrated solution

GEIS provides users, through transparent single sign-on (SSO), a secure entry-point to common GIAC business applications (i.e. electronic time and expense reporting), content repositories, email, and search engines. For both internal and remote users, GEIS serves as the front door of authentication and access control, with RSA SecurID providing strong authentication to validate remote user identity, and RSA ClearTrust authorization providing the user privilege management capabilities that control what resources users are able to

[5] Plumtree Software Home Page. *17 Jan. 2003. <http://www.plumtree.com/customers/industries/pharmaceuticals_healthcare/pharmacia.asp>.*
[6] Perseid Software Limited.

access. ClearTrust provides access control based on either basic entitlements (ACLs) or its SmartRules capability where access is granted on a business decision/rule. This provides a two-factor authentication solution that is designed to protect the network and the data integrity. Further, the combination of two-factor authentication and role-based access management, audit and administration functions should position GIAC to exceed some of the key security and privacy guidelines under HIPAA.

For remote access, the user must present two identification factors: with a SecurID token device and the users' individual PIN code. SecurID token devices generate a new, random number code every 60 seconds. This code, along with a user-assigned pin code, forms a dynamic "passcode", which a user enters as their password. User passcodes are verified by the RSA ACE/Server at the Boston data center. The RSA ACE/Server functions as a back-end security server, authenticating and recording all user requests for access to protected resources.

Local domain access is managed through standard Windows 2000 Active Directory authentication controls. Once authenticated to the domain, data and application access is centrally managed through ClearTrust, which synchronizes with the Lightweight Directory Application Protocol (LDAP) repository. When a user makes a request for the GEIS Home URL through his/her browser, he/she will be prompted with a ClearTrust Login Screen. When any user, local or remote, authenticates to ClearTrust, the username is extracted from the HTTP headers and passed onto Plumtree for SSO.[7] After the user successfully authenticates, they will be redirected to their GEIS portal home page. The ClearTrust username and the Plumtree username will be one and the same since they are both synchronizing with the same LDAP directory.

From the GEIS portal home page, users access applications through Plumtree portlets. Microsoft Exchange portlets, for example, display email, contact and calendar information centrally on a web page. The Microsoft Exchange portlets run on servers separate from the portal's main application server, to isolate resource-intensive processing and to limit conflict with other portlets as well as with other GEIS components. The portlets are Active Server Pages that use Microsoft Collaborative Data Object technology to communicate with Exchange. Plumtree stores user log-in information and profile data, freeing GEIS users from having to re-login to Exchange for each GEIS session.

The GIAC business model incorporates additional collaborative technologies using the Internet based GroupSystems OnLine applications suite to increase R&D innovation, reduce product development cycles, and facilitate overall business communication. Scientists (biologists, pharmacologists and chemists), clinical development professionals, and project managers bridge geographic boundaries working in "team" R&D efforts through web-based collaboration and with decision-making applications. Managers use decision-

[7] Plumtree Software Home Page. "RSA ClearTrust Ready Implementation Guide For Portal Servers and Web-Based Applications". 13 Nov. 2002. 18 Feb. 2003. <http://rsasecurity.agora.com/rsasecured/guides/cleartrust/Plumtree_Corporate_Portal_v4_5_CT50.pdf>

making tools for strategic planning and other key business processes reducing travel costs and down-time of key personnel. Users conduct virtual meetings, "sometimes in a facilitated environment". Personnel connect remotely from approved PCs using GroupSystems client software to the GroupSystems server located inside the corporate firewall. The GroupSystems applications are used exclusively for personnel activities, with one exception. GIAC uses the GroupSystems Survey tool to publish consumer surveys on the external web site. Surveys are customized from a GroupSystem client PC, and published from the GroupSystems server, via Web server connection. Consumer responses do not return to the GroupSystems server, but are directed to the Oracle database where results are compiled for analysis.[8]

GroupSystems is not accessible through GEIS, and has an added authentication mechanism. User IDs and passwords are selectively issued on as needed by a GroupSystems System Administrator, and are always separate from other network resource IDs. Approved personnel gain secure remote access to GEIS and GroupSystems Applications through SecurID and Windows 2000 authentication. Internally, the process is the same, with exception of SecurID authentication.

All GIAC personnel are issued desktop PCs on the private network, each managed and configured by ITMD staff. Only ITMD personnel have administrative privileges on workstations, thereby preventing installation of unlicensed or unauthorized software. Personnel are not authorized to access GIAC resources remotely from personally owned computers, whether desktop or laptop. Those requiring remote access must use laptops managed and configured by ITMD staff. The standard laptops configuration consists of the Cisco VPN client for Windows 2000 with the credentials needed for a secure IPSec connection to the GIAC network.

The public Web server functions to establish GIAC's public presence, primarily for marketing, while the internal Web servers support various internal business applications. Internal Web servers are isolated from the Internet by stateful firewalls within the DMZ. Reverse proxies divert communication between the Internet and GIAC's external Web site. The external Web server resides within the DMZ.

GIAC hosts its Exchange 2000 e-mail server within the private network at the Boston office. Policy Patrol Enterprise[9] is installed on the Exchange server for virus checking, keyword filtering, and attachment blocking, as well as policy management. Policy Patrol rules are configured and enforced based on GIAC e-mail policy. Since social engineering threats are a particular concern for GIAC, many rules are configured to address those threats (i.e. spoofing attacks). Keyword filtering is enabled to detect sensitive (trade secret) data passed in email text and attachments. Re-offending virus senders are blocked. Messages

---

[8] "Dispersed and Global Project Teams." *groupvision Switzerland.* <http://www.groupvision.ch/services/text/2-imeetings.htm >

[9] Red Earth Software Homepage. 19 Feb. 2003. <http://www.redearthsoftware.com/PolicyPatrolEnterprise.htm#Virus_scanning>

containing viruses or malicious code are quarantined.

GIAC's data backup and restore strategy includes normal (full) backups of DNS, Sendmail, GroupSystems, Plumtree, and Web servers occur weekly. Exchange Server and Oracle databases, because of the "mission-critical" nature of the data they contain, are backed up on a daily, incrementally basis – that is, normal backups are performed on the first day of the backup cycle, and incremental backups are performed on following days. An alternate data integrity measure, critical data is sent in real time to a hot standby site using a Cisco MPLS and VPN site-to-site strategy, to provide for offsite recovery.

Although GIAC applications lend value to operational efficiency, none are deemed "critical" in terms of availability – that is, temporary down-time.). However, certain applications, because of the nature of the information in them, where confidentiality and integrity are greater concerns to GIAC, require special management oversight and are treated as critical. Portal, Intranet applications, and backend databases, for instance are considered equally critical in terms of data confidentiality and integrity– that is, each handle sensitive information that if compromised, could result in theft of proprietary information, damaged reputation, and legal liabilities for noncompliance where privacy regulations exist.

Critical Risk Areas

GIAC's greatest concern is the confidentiality of their R&D information. Data integrity is also high on the list because data loss or corruption could result in a significant amount of lost time, have serious impact on research efforts, and ultimately impact market position in this highly competitive sector. Based on the priorities set by GIAC, the following is a very high-level priority list of the goals that GIAC's security policy should strive to achieve: confidentiality, integrity, and availability. Keeping these goals in mind, three critical risk areas are defined based upon relative threat measurements: The criticality of various assets effected, the likelihood of threat occurrence, and the impact on GIAC business operations.

Trade Secret Misappropriation

Threat or Risk Overview

Trade secret misappropriation is a risk whereby an offender, sometimes with the aid of unknowing assistants, might obtain and convert a trade secret, with the intent to deprive GIAC (the owner) of its use in order to gain economic benefit. A "trade secret" is generally defined by the Uniform Trade Secret Act (USTA) as:

> Information, including a formula, pattern, compilation, program, device, method, technique or process, that: (1) derives independent economic

value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

"Misappropriation" is defined by the USTA as:

(1) The "[a]cquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or (2) disclosure or use of a trade secret of another without express or implied consent by a person who (a) used improper means to acquire knowledge of the trade secret; or (b) at the time of disclosure or use knew or had reason to know that his knowledge of the trade secret was (i) derived from or through a person who has utilized improper means to acquire it; (ii) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or (iii) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or (c) before a material change of his position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake."

In this context, "improper means", according to the USTA, includes "theft, bribery, misrepresentation, breach or inducement of a breach of duty to maintain secrecy, or espionage through electronic or other means."

Threat Significance to GIAC Enterprises

At GIAC, R&D activities consume more than 60 percent of the annual budget. Millions are invested annually with high hopes of eventually recouping that investment in the form of a New Chemical Entity (NCE), or even better—a blockbuster cure for cancer. "The typical new drug, brought successfully to market, costs approximately $600 million for research and development." [10] Patent protection of the NCE will afford GIAC exclusive rights to market the drug for 10 years. The incremental sales over this period are projected not only to recoup the initial R&D investments, but will provide the means to satisfy the financial community's demands for business growth.

The most critical item to the continued operations and success of GIAC (its "crown jewel") is its intellectual property—specifically, the trade secrets--the compounds and formulas that comprise potential NCEs. Unlike most intellectual property (patents, trademarks and copyrights), there is never a registration or certificate informing third parties that a business is claiming information as a trade secret. The only certain way to establish what information is a trade secret is by a court ruling.[11]

---

[10] Kettler, Hannah. "Updating the Cost of a New Chemical Entity." 11 Dec 2002. 17 Jan 2003. <http://www.ohe.org/updating.htm>

[11] Weil Gall, Barbara. "An Overview of Intellectual Property Protection." *GigaLaw.com.* Oct. 2000. 19 Jan. 2003

Feasible Consequences and Likelihood of Vulnerability Exploit

Potential Threat Agents/Events

According to an ASIS Survey cited by Kevin Johnson, 60% of a pharmaceutical company's threat profile consists of its employees (current, former, retired, or part-time); 15% from vendors, consultants, joint venture partners or subcontractors; and, 25% from outside professionals (foreign and domestic, legal and illegal).[12] Trade secrets are as vulnerable to the common threat agents (accidental, natural, or deliberate), as most assets. Since trade secrets are coveted and sought by competitors and opportunists, a focus on espionage threats, both external and internal agents, as well as the methods and technologies to facilitate events seems a logical approach.

Increasingly, and especially in the pharmaceutical industry, management strategists are relying on a "frequently misunderstood practice known as Competitive Intelligence" (CI). In effect, CI is corporate espionage with a new twist, in which its professionals "legally and ethically collect, analyze, and apply information about the capabilities, vulnerabilities, and intentions of their competitors, and monitor developments within the overall competitive environment (such as previously unseen rivals over the horizon, or new technologies that could change everything)". The goal: actionable intelligence that will provide a competitive edge.[13] Consider the possibility of a less scrupulous CI analyst, whose actionable intelligence sought might include GIAC trade secrets--perhaps an un-patented NCE formula. So, how do "ethical spies" gather intelligence? Here are a few, of the many techniques they might employ at GIAC:

- Social engineering tactics, both public and private
- Creating psychological profiles of GIAC executive decision makers
- Mining and analyzing data already in operational files
- Technology scouting via patent tracking and other tools that reveal areas in which competitors are likely to make breakthroughs
- Attending trade shows and conferences smartly, and so on [14]

The Society of Competitive Intelligence Professionals (SCIP), a global, non-profit organization, promotes compliance with U.S. and International laws relative to the CI practice (i.e. The Economic Espionage Act of 1996 (EEA) with articles, resources, as well as established ethical guidelines of its own.[15] For those "good old-fashioned" corporate espionage practitioners, who by ignorance or choice, are unconstrained by the EEA, the threat takes on a new form with alternate means of acquiring trade secrets and related sensitive material.

<http://www.gigalaw.com/articles/2000-all/gall-2000-10-all.html>

[12] Johnson, Kevin. "Security of Pharmaceutical Intellectual Property in the Era of Electronic Regulatory Submissions." 2000. 17 Jan 2003. <http://www.pharmaknowledge.com/Security%20-%20KJohnson%20presentation.pdf>

13 Johnson, Kevin.

14 Johnson, Kevin.

15 The Society of Competitive Intelligence Professionals (SCIP) Home Page. 18 Jan. 2003. <http://www.scip.org/index.asp>

Human threat agents--spies, attackers, or “agents”, as they are hereafter referenced--operate from inside and outside the company. They may be competitors, third-party business partners, vendors, contractors, hired spies, as well as disgruntled, bored, or naïve employees. Because agents must have access to information resources and insiders generally have easier access than outsiders, GIAC’s greatest enemies are their own personnel: some with devious or opportunistic agendas, and others who are simply “clueless” event facilitators.

In § 1832 of the EEA, “trade secret theft” is exhaustively defined by five elements, each of which provide a good basis to categorize the tactics used to commit the crime. Associated with each element below is an example of common tactics used to obtain sensitive information. Note that some of the tactics may apply to multiple elements, though mentioned only once, and that only one example is provided for each, although the possibilities are innumerable.

”…(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;”

- Social engineering. Example: An agent masquerading as a GIAC senior executive places a frantic call to a help-desk employee, claiming to have forgotten his password. The help-desk employee, confused and intimidated by angry threats, quickly divulges the executive’s network logon password to the agent, who uses this information to access the GEIS R&D database.

“(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;”

- Electronic eavesdropping. Example: An internal agent, posing as the facilities staff responsible for tracking GIAC equipment assets surreptitiously places electronic data gathering devices (keystroke capture devices, digital phone/FAX recording devices, miniature video capture devices) throughout a research laboratory and its adjoining conference room.

“(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;”

- Bribery. Example: An agent, after having profiled personnel, approaches the employee with a generous cash offering in exchange for a NCE formula.

“(4) attempts to commit any offense described in paragraphs (1) through (3); or “

- Hacker intrusion. Example: An external “spy” or intruder attempts to gain access to GEIS R&D data by packet sniffing, using password crackers,

Trojan horses, and/or backdoors.

"(5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3)…"

- Group collusion. Example: A few GIAC employees conspire together, using their collective knowledge and privileges to gain access to information.

These are only a sample of possible means to attempt access to sensitive information or trade secrets. Among other threats GIAC should consider are: some of the other numerous examples those include:

- Dumpster diving. A dirty job, but a great way to find valuable information if carelessly disposed by a careless or naïve GIAC employee.
- Non-standard software that has not been tested for potential exploits.
- User's private network compromised and used to gain access to the corporate resources (i.e. telecommuters).
- Unauthorized modem use via personal dial-up accounts as possible entry point to the internal network.
- Laptop theft.
- Simple personnel "cluelessness". For example, an employee may post a resume on the Internet that discloses in the "Accomplishments" section a highly confidential R&D project on which the employee is working.

Likelihood of the Event(s)

Moderate. Clearly, computer-based systems can abet personal misbehavior or accidental harm, leading to trade secret disclosure or harmful data modification. Without access controls, the careless or unprincipled person can be provided with easy access to large amounts of sensitive information and trade secrets. The likelihood of events facilitated by human error, carelessness and lack of awareness is moderate, but may depend upon personnel awareness of information sensitivity and handling policies and procedures. The likelihood of such events facilitated by disgruntled personnel, contractors or consultants is likely higher, and more so when they are later employed by a GIAC competitor.

Impact of Event(s)

Severe. A trade secret exploit, while not the most likely to occur, ranks as the most significant in terms of severity for its impact on profitability and survivability.

Consequences of Event(s)

The most obvious consequence is the potential loss of profitability and recouping of R&D investments if a NCE formula were misappropriated by a competitor. The competitor might develop the blockbuster cure for cancer, obtain

patent protection and approval from the FDA and reap all the benefits. To challenge the trade secret misappropriation spawns a new risk of its own. As the plaintiff, GIAC would have the burden of proving that the information qualified as a "trade secret" as defined by law, and that the measures taken to protect the information in question were "reasonable" under the "totality of the circumstances" (i.e. value and importance of information, size of company, etc.). Regardless of the outcome, the litigation process would be burdensome and expensive.

Steps to Mitigate the Risk

Protecting trade secrets is not only a difficult technical challenge, but is also a human endeavor that is highly dependent upon the behavior of individual people. GIAC should incorporate this doctrine in its risk management program as an overall mitigation strategy. "A good program should include premises security, control of confidential information, non-disclosure agreements with third-party business partners, and employment agreements that prevent disclosure of confidential information."[16]

The most effective means of protecting GIAC sensitive information is through selective dissemination – making information resources available on a "need to know basis" using physical and system-based access controls. With access controls in place, an audit policy should be established for monitoring system–based access. The Information Sensitivity or Data Classification policy should establish the "foundation for the audit policy", the information classification scheme to be used, and how it is to be applied.[17]

As stated later in this paper, only by categorizing data according to its sensitivity to loss or disclosure can GIAC implement proper controls with respect to disclosing information. A well-defined Information Sensitivity policy, coupled with a good personnel awareness program will reduce "human factor" risks through awareness of data handling requirements. One cannot secure data if one does not understand the value of that data. Data handling procedures will further reduce "human factor" risks.[18]

Finally, but of equal importance, focus should be applied to GIAC's hiring practices, particularly personnel candidate screening. By conducting careful background checks, psychological interviews, personality tests and drug tests, important personal behaviors and character issues can be revealed. Reviewing one's work history and references will not reveal sufficient insight to gauge a person's trustworthiness.

There are numerous measures that GIAC can take to reduce this threat. Many safeguards have already been implemented within GIAC's current hiring

---

16 Weil Gall, Barbara. "An Overview of Intellectual Property Protection." *GigaLaw.com.* Oct. 2000. 19 Jan. 2003 <http://www.gigalaw.com/ articles/2000-all/gall-2000-10-all.html>

17 Chapple, Mike; Shinder, Deborah; Tittle, Ed. "TICSA Certification: Information Security Basics." InformIT.com 22 Nov. 2002. 18 Jan. 2003. <http://www.informit.com/isapi/product_id~%7BE9081702-D789-4795-B7DE-6315866D67CC%7D/element_id~%7B4C230C18-7506-49E7-95F9-A0F00C7A7F1E%7D/st~%7B5947591F-62F3-4B59-B9CC-35BAC4E3C229%7D/content/articlex.asp>

18 Itlillious, Inc. Home Page. "Iris & Itlillious' Security Awareness Portal" 3 Mar 2003. <http://www.itillious.com/iris/dataclass.html>

practices, employment policies, approved LAN and Computer usage Policies, distributed work flows, as well as the organizational and work flow separation built in to the current IT infrastructure. Table 1 lists several candidate mitigation steps worth considering.

Control Type	Candidate Mitigation Steps
Physical	▫ Institute overall physical security precautions, such as fencing the perimeter of the company premises, limiting the number of entrances and exists, using alarmed or self-locking doors, and hiring after-hours security personnel. ▫ Place biometric devices (i.e.retina scanners) at entries to labs, data centers, and other "sensitive" areas. ▫ Store NCE formula or equally sensitive information only on stand-alone PCs with no connection to any other computer or phone line. ▫ Lock or bolt all computer hardware to the floor, wall or a large piece of furniture. ▫ Employ device tagging stickers and an equivalent inventory tracking system. ▫ Employ surveillance detection mechanisms in sensitive work areas
Technical	▫ Implement Role-Based Access Control (RBAC) for GEIS and all GIAC information systems—base access on job function and need to know. ▫ Conduct regular system vulnerability scans. ▫ Compare quarterly scans with an independent baseline developed by a an independent security firm for validation and integrity purposes. ▫ Employ a PKI-based email solution for tracking, verification, non-repudiation and authenticity purposes
Administrative	▫ Develop clearly written information sensitivity level policies and procedures. ▫ Develop a robust personnel screening and risk management program including background checks on all prospective personnel, contractors, and others having unescorted access to GIAC facilities. ▫ Develop procedure for safeguarding confidential information by its established sensitivity level. ▫ Incorporate into security awareness program, an emphasis on handling sensitive information, individual employee responsibility for protecting the information, etc. ▫ Enter into confidentiality and nondisclosure agreements with employees, independent contractors and temporary personnel, suppliers, customers, potential business partners, and third parties. ▫ Develop procedures for unfriendly termination. Consider the prompt removal of system access and in some cases, the physical removal from the offices.

Table 1: Recommended Mitigation Steps

Potential Civil or Criminal Liability

Threat or Risk Overview

The business impact of risk management, or lack of it, makes IT security an issue that extends beyond GIAC's infrastructure and applications. In the context of information security, civil and criminal liability threats often arise where "due care" and "due diligence" are not adequately exercised, and mostly pertain to the preservation of security and privacy of individuals. "Due diligence" and

"due care" relate to the common law concept of "negligence", which Black's Law Dictionary defines as "[t]he omission to do something which a reasonable man guided by those ordinary considerations which ordinarily regulate human affairs would do, or the doing of something which a reasonable and prudent man would not do." [19]

Due care means to avoid acts or omissions, reasonably foreseeable that would cause "injury" (i.e privacy disclosure). Due diligence is simply the management and execution of due care. Due diligence is the opposite of negligence. For example, GIAC could be considered negligent if it were to be found in breach of its duty to exercise due care and an injury occurred as a result of the breach.

Threat Significance to GIAC Enterprises

As a pharmaceutical company whose research and products impact the health and lives of many people, liability risks are inherently significant. As a "covered entity" under the Health Insurance Portability and Accountability Act (HIPAA) of 1996, GIAC has the added liability to protect the privacy and integrity of individual patient health information that is stored in electronic and paper formats, including all copies, backups and archival data.

> HIPAA is designed to protect confidential healthcare information through improved security standards and federal privacy legislation. It defines requirements for storing patient information before, during and after electronic transmission. It also identifies compliance guidelines for critical business tasks such as risk analysis, awareness training, audit trail, disaster recovery plans and information access control and encryption.[20]

Liability risks are increasing in significance to GIAC as the U.S. Government has begun to more rigorously enforce the patient privacy laws that apply to the pharmaceutical industry. Until recently, the majority of the government's enforcement efforts have focused on health care providers. Now pharmaceutical companies like GIAC are finding themselves under scrutiny – with senators and congressmen calling upon the FTC to monitor pharmaceutical marketing practices that may violate patients' privacy.

Feasible Consequences and Likelihood of Vulnerability Exploit

Potential Threat Agents/Events

The "threat of errors and omissions by employees account for more losses than deliberate acts; therefore they should be the focus of attention". [21] Equally, deliberate threat agents and various exploit methods should not be overlooked. In one scenario, an employee may access and manipulate clinical trial or patient records databases… the possible outcomes are innumerable – and the access

---

[19] Black, Henry C. Black's Law Dictionary. 6th ed. New York: West Group, 1990. pg. 1032.

[20] Rx2000 Institute Home Page. "Health Insurance Portability and Accountability Act (HIPAA) Frequently Asked Questions." 16 Jan. 2003. <http://www.rx2000.org/KnowledgeCenter/hipaa/hipfaq.htm#Intro>

[21] Erwin, Dan. "e-risk, Liabilities in a Wired World." *Computer Security Alert*. Aug. 2000. 17 Jan. 2003. <http://www.gocsi.com/pdfs/erisk.pdf>

may have been accidental – or maybe not.

Some HIPAA requirements create significant barriers for researchers needing access to patients and or their information for research recruitment.

> Under HIPAA a covered entity "[m]ay not use or disclose identifiable health information (PHI) for research purposes unless the patient has authorized the disclosure pursuant to a HIPAA valid authorization, or a waiver of authorization has been granted by an IRB or Privacy Board."

The GIAC researcher, frustrated by the challenge of simply finding willing research participants, *intentionally* circumvents the HIPAA "red tape" to make his job easier. Without understanding or appreciating the rationale behind the regulation, a researcher might only see the "hurdle" it represents. This scenario represents an intentional threat without malicious intent.

Again, human error and carelessness pose the greatest risks of disclosure. These scenarios are innumerable.

Likelihood of the Event(s)

High. As stated previously, GIAC personnel (including contractors), whether acting intentionally or unintentionally, are likely to pose the greatest number of liability related threats. According to Kevin Johnson, however, it is the "naïve employee" who poses the greatest threat in the pharmaceutical industry.[22] Based on this reason, it may be reasonable to assume that the likelihood of security breaches would be high.

Impact of Event(s)

Low to Moderate. The severity of event impact will depend upon what is breached or violated. At a minimum liability threats can lead to business interruption, confusion and distraction among personnel, and adverse publicity. At worst they can result in compromising patients' safety, expensive and protracted litigation, interruption of production, being shut down temporarily or permanently, imposition of serious damages and, if pursued as a criminal matter, potential jail sentence risks for the company's management team, and exposure of the company and its executives personally to multimillion-dollar fines.

If GIAC fails to comply with HIPAA, it faces the risk of penalties and increased government scrutiny. Perhaps most importantly, they risk the permanent loss of trust from increasingly demanding health care consumers.

Consequences of Event(s)

Again, consequences will depend on what was breached, and what damages resulted, among other variables. Under HIPAA for example, if GIAC were found liable for a security compromise, it can face hefty criminal penalties

[22] Johnson, Kevin.

and sanctions—up to 10 years in prison and/or a $250,000 fine. Even if GIAC were determined not criminally liable, it would still be subject to civil liability. But the civil remedies of $100 per violation, with a $25,000 cap per calendar year for each provision violated, are probably trivial compared to the bad press that would likely ensue.23 Such disclosure might lead to harm in the company's status and reputation with investors, competitors, and the public.

Steps to Mitigate the Risk

GIAC must be able to demonstrate due care and due diligence by ensuring that its risk management program (1) complies with all legislative mandates; (2) implements steps necessary to protect its assets, and (3) and remains a continuous endeavor to ensure that the appropriate protective mechanisms are in place, and adjusted as necessary. Reviews should take place at least bi-annually, to ensure that measures are still consistent with business goals, new legislative mandates, technologies, threats and exploits.

Again, GIAC has already implemented several safeguards within its IT infrastructure: Microsoft Terminal Services, SecurID authentication, Cisco IDS Module, Cisco VPN. Additionally, planning has already begun to meet the April 13, 2003 compliance deadline. All plans will be documented and evaluated against the compliancy regulations within the Human Resources and Legal Divisions to determine the appropriate course of action that must take place. Upon subsequent investigation, policies and practices will be employed to meet the guidelines outlined by HIPAA within GIAC and it's corporate endeavors. This will include Policies, practices and business models that are currently utilized within GIAC's culture, but not be limited to procedure only, specific recommendations for the network and data management aspects of GIAC will evolve and be modified from this effort.

A data classification policy is fundamental to HIPAA compliance, as is likely the case with other laws. Ad-hoc approaches to determining value, risk, and protective measures cannot be adequately defended. Training is also key to implementing a data classification policy – to educate personnel on what needs protection and how, as well as defining responsibilities for protecting data.

"Due care" can further be met by implementing the following suggested mitigation steps (see Table 2).

Control Type	Mitigation Steps
Physical	▫ Place biometric devices (i.e.retina scanners) at entries to labs, data centers, and other "sensitive" areas.
Technical	▫ Implement Role-Based Access Control (RBAC) for GEIS and all GIAC information systems—base access on job function and need to know. ▫ Develop a process that requests, establishes, issues, and closes user accounts; and tracks users and their access authorizations. ▫ Encrypt data on laptop hard drives using stand-alone encryption product that integrates with the laptop. ▫ Encrypt data in transit.

[23] Harris, Shon. CISSP All-in-One Certification Exam Guide. California: McGraw-Hill/Osborne, 2002. p. 862

Administrative	▫ Ensure that employee laptops are hardened and configured to prevent changes by the user, with AV software installed. ▫ Conduct regular system vulnerability scans. ▫ Employ a PKI-based email for tracking, verification, non-repudiation and authenticity purposes. ▫ Establish an employee information security awareness and training program that becomes an integral part of the corporate culture ▫ Develop clearly written information sensitivity level policies and procedures. ▫ Develop procedure for safeguarding confidential information by its established sensitivity level. ▫ Incorporate into security awareness program, an emphasis on handling sensitive information, individual employee responsibility for protecting the information, etc. ▫ Develop procedures for unfriendly termination. Consider the prompt removal of system access and in some cases, the physical removal from the offices. ▫ Develop procedures for outgoing or transferring employees. The removal of access privileges, computer accounts, authentication tokens. The control of keys, the briefing on the continuing responsibilities for confidentiality and privacy, return of property, and the continued availability of data the employee may have filed. ▫ Improve GIAC's overall business model and operational practices by incorporating the following standards and guidelines: ▫ ISSO CMM Practices ▫ ISO 9000 Quality Management Principles ▫ ISO/IEC17799 Code of Practice for Info Security Mgmt

Table 2: Recommended Mitigation Steps

Compromise of System / Data Integrity

Threat or Risk Overview

IT security vulnerabilities are a source of avoidable costs for business — whether due to loss of productivity resulting from a virus outbreak,

Threat Significance to GIAC Enterprises

As addressed above, current FDA regulations, under Title 21 of the CFR, require pharmaceutical companies to implement procedures to ensure the authenticity and integrity of electronic records, including limiting computer access to authorized individuals and keeping audit trails of computer activity.

Feasible Consequences and Likelihood of Vulnerability Exploit

Potential Threat Agents/Events

Cyber crime is a common threat in which the attacker uses network access to commit a criminal act. With the exponential growth of Internet connections, the opportunities to exploit network weaknesses are multiplying. Attacks may be internal or external, with the former being easier to perpetrate.

- "Back doors" or "maintenance hooks" remaining in the production system for an internal attacker to exploit at a later time.
- Failing to update the virus definition files on a regular basis increases the risk of infection from a variant for which you do not have the necessary vaccine. This can cause great damage.
- A failure to run regular virus scans across all data files on GIAC's server(s) reduces the ability to detect and cure a virus before its 'footprint' is identified by a GIAC employee user trying to open the file in question.
- A lack of user awareness about the risks involved in opening unsolicited e-mails may result in a virus infection spreading throughout GIAC's organization.
- Criminals may target GIAC's information systems, resulting in serious financial loss and damage to GIAC's business operations and reputation.
- Web server(s) may be subjected to a DoS attack, which could result in business interruption and financial loss.
- Self-propagating malicious code, downloaded by the unwitting employee will cause damage not only to GIAC's system, but can continue to wreak havoc as it spreads to other organizations and individuals.

Of course, there are many other threat agents, but the focused on here is foremost in the minds of of the people responsible for the company's assets.

Likelihood of the Event(s)

High. Based on responses from computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities, the findings of the "2002 Computer Crime and Security Survey" confirm that the threat from computer crime and other information security breaches continues unabated and that the financial toll is mounting.[24] Cyber Crime seems likely to rise, according to Stephen Lukasik, a visiting scholar at CRISP. "We're beginning to notice that water is rising, but we don't see the flood. We're going to run out of cops and courts before we run out of crooks."[25]

CRISP conducted an independent poll and found that Ninety percent of respondents in 2002 (primarily large corporations and government agencies) detected computer security breaches within the last twelve months. Eighty-five percent detected computer viruses; 35% suffered unauthorized access or misuse on their Web sites within the last twelve months; 21% said that they didn't know if there had been unauthorized access or misuse.[26]

Impact of Event(s)

Moderate to High. Because R&D efforts are inherently time-intensive, if data were either lost or corrupted (assuming that there is no way to retrieve the

[24] "2002 Computer Crime and Security Survey". *Internet Psychology Research Institute (IPRI) Home Page.* 19 Jan. 2003. <http://www.internet-psychology.org/efraud/computer-crime.htm>
[25] "ERA Commons". *Computer Retrieval of Information on Scientific Projects (CRISP) Home Page*. 18 Jan. 2003. <http://crisp.cit.nih.gov/>
[26] Computer Retrieval of Information on Scientific Projects (CRISP) Home Page.

data) in a successful attack, it is almost certain that the business would be heavily impacted by the time and effort set-back. In less likely scenarios, an attacker's false manipulation of data may create high impact resulting in improper medical treatment and ultimately patient death or moderate impact resulting from creating and revealing fatal deficiencies in the compound screening prior to clinical trials. In any event, either scenario may lead not only to civil and criminal penalties, but to public embarrassment and financial loss as well.

Consequences of Event(s)

Data integrity exploits could result in a range of costly consequences for GIAC: loss of life, loss of dignity, loss of time or loss of employment. Notwithstanding violation issues, problems with data integrity, patient protections, fraud, etc., raise questions about the very mission of pharmaceutical companies, particularly those emphasizing the quality of their R&D/science capability. Other possible consequences include:

- Shortage of patients
- Delays in/withdrawal of product approval (can cost companies hundreds of millions or even billions of dollars in lost revenue)
- FDA-imposed holds on clinical trials
- Withdrawal of approval after a product is on the market[27]

Steps to Mitigate the Risk

Maintaining patches is the single most effective, inexpensive, and easy to implement step that administrators can undertake to secure their networks. Vendors will typically provide accumulative OS patches and known bug fixes for security problems, which can be loaded separately from the application.

Personnel security plays a role in mitigating this risk as well. Develop procedures for outgoing or transferring personnel. The removal of access privileges, computer accounts, authentication tokens. The control of keys, the briefing on the continuing responsibilities for confidentiality and privacy, return of property, and the continued availability of data the employee may have filed.

Develop and implement stringent password policies and procedures, stipulating that passwords: (1) be at least 8 characters in length; (2) contain a combination of alphabetic, numeric, and special characters; (3) contain a non-numeric in the first and last position; (4) contain no more than 3 identical consecutive characters in any position from the previous password; (5) not contain dictionary words in any language; (6) not contain any proper nouns or names of any person, pet, child, or fictional character; and (7) not contain any personnel serial number, Social Security number, birth date, telephone number, or any information that could be readily guessed about the creator of the password.

Another critical measure to protect data integrity is to ensure that

[27] Swiatocha, Michael. "Conducting a Clinical Compliance Risk Assessment in the Pharmaceutical Industry". 25 Mar. 2002. 11 Jan. 2003. <http://www.ehcca.com/presentations/ressummit2/3_03.pdf>

hierarchical backups are performed on a daily basis. One effective backup scheme involves three redundant copies of backups over a given period of time. The idea is that a tape is not returned to the reuse stack until it is the fourth tape in a given series. A series consists of daily backups, weekly backups, and monthly backups. A level 0 backup is a complete copy of the entire file system. This may be performed monthly, in which it is part of the scheme, or on both a periodic and an as-needed basis. For example, the optimal time to perform a level 0 backup of the operating system is when changes are made to the OS files. Periodic checks of the backup tapes should be made to ensure that they contain valid data. This will prevent an unrecoverable emergency when a restore must be performed and the tape contains bad or no data. Table 3 provides some additional suggested steps.

Control Type	Mitigation Steps
Physical	▫ Ensure that the systems that comprise the network (such as file servers, Web servers, mail servers, and any other equipment that forms the basis of the network) will be secured in an area where access is controlled. ▫ Implement door delay system in controlled areas. ▫ Use laptop device locks for telecommuters.
Technical	▫ Perform hierarchical backups on a daily basis. ▫ Employ cryptographic based electronic signatures. ▫ Maintain OS patches and bug fixes. ▫ Conduct regular system vulnerability scans. ▫ Review audit logs. ▫ Disable unnecessary services. ▫ Modify registry access permissions to allow only SAs to access certain entries. ▫ Periodically review user account management on a system, i.e., are accounts still active, has training been completed. ▫ Set up administrator accounts for individual administrators. ▫ Update anti-virus software. ▫ Employ a PKI-based solution for all electronic transactions for tracking, verification, non-repudiation and authenticity purposes
Administrative	▫ Develop and implement stringent password policies and procedures. ▫ Develop and implement a strong security awareness and training program, educating users of potential threats. ▫ Granting access should be based on separation of duties and least privilege. ▫ Verify the need for modems; remove them if they are unnecessary. ▫ Ensure separation of duties to divide roles and responsibilities so that a single individual cannot subvert a critical process.

Table 3: Recommended Mitigation Steps

Evaluate and Revise Security Policy

This section provides the evaluation, analysis, and customized revision of a model (template) Information Sensitivity Policy, based upon its relevance to the confidentiality risks and disclosure threats pervasive throughout GIAC's key risk areas identified above. This "Information Sensitivity Policy" might also be called

a Data "Classification" or "Categorization" Policy, as they generally serve the same purpose. For the purpose of this assignment, the terms may be used interchangeably.

Only by categorizing data according to its sensitivity to loss or disclosure can GIAC implement proper controls with respect to disclosing information. Based on this categorization, policies for consistent information handling can be defined. Effective data classification policies and procedures reduce risk by improving awareness, establishing employee accountability for unlawful breaches of confidential information; and determining how data will be secured, managed, retained, and disposed of. Additionally, data classification is fundamental to complying with HIPAA, and other privacy-related laws. The revised version of this policy will specifically address issues relating to trade secret misappropriation and privacy-related civil or criminal liability risks discussed in the previous sections.

Evaluate Model Information Sensitivity Policy

While the SANS Information Sensitivity Policy is not an actual policy, its template provides an excellent starting point in developing a customized policy to address GIAC's unique business needs. The model is logically structured, well written, and addresses most issues that should be incorporated in an issue-specific policy of its kind.

For the purposes of evaluating the model Information Sensitivity Policy, issues will be addressed by sections will be referenced by the section title/sub-title name and/or the corresponding section number. For the full and complete text version of the model SANS Information Sensitivity Policy, refer to Appendix A.

The model Information Sensitivity Policy is structured in the following manner:

- Purpose
- Scope
- Policy
- Enforcement
- Definitions

The "Purpose" section states the intent of this policy, which is to "help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside the organization without proper authorization". This section lightly addresses issues related to information labeling and handling, and sensitivity level definition guidelines.

The "Scope" section addresses the breadth of scope pertaining to information assets by relative sensitivity level, as well as the employees' responsibility to protect them. The section defines the primary categories, "Public" and "Confidential", citing a range of examples. The information handling

guidance provided leaves much to interpretation, and is not adequately descriptive for GIAC's purposes. "<Company Name> personnel are encouraged to use common sense judgment in securing <Company Name> Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager."

The policy statement, or "Policy" section states the guidelines in detail on how information should be protected according to its sensitivity level. Information is broken down into three sensitivity levels: "Minimal Sensitivity", "More Sensitive", and "Most Sensitive", in subsections 3.1, 3.2, and 3.3 respectively. Within each subsection are guidelines for handling information at its respective sensitivity level. These instructions provide basis for individual decisions and actions within the scope of handling, distributing, and storing information. The instructions also include "Penalties for deliberate or inadvertent disclosure" of sensitive information. While the instructions in the model are comprehensive and thorough, some will naturally require revisions to place more emphasis on trade secret and patient heath information issues.

The "Enforcement" section simply states the possible consequences of violating the policy.

The final section, "Definitions", states meanings for terms used throughout the policy, and provide some detailed guidance on what actions are to be performed.

The model policy does not contain a "Background" section, nor is much "background" revealed anywhere in the document to expand upon the purpose statement and provide additional reasoning for following through on implementation of this policy.

The model policy lacks a "Responsibility" section, but vaguely addresses "employee" responsibility in carrying out selective directives in the "Purpose" and "Policy" sections. It does not indicate who is responsible for implementing the policy, or provide information on who can draft, approve, or modify the policy.

The model policy also lacks an "Action" section but does define what things are to be accomplished within the "Policy" section. There are no references to when or how frequent actions are to be accomplished.

Overall, the model policy is a good framework from which to build an Information Sensitivity Policy, particularly for its well-constructed "Policy" section. It is easy to read, and logically covers the scope of guidance that it should contain. As a model, there are many issues and details that it cannot provide because it is simply that—a template. Its shortcomings are primarily that it does not, even in the generic sense adequately address the risks that it is designed to protect against, or assign responsibility for those who will be integral to the implementation and continuity of the policy. Much Revision is necessary to fit GIAC's scenario.

GIAC Enterprises Information Sensitivity Policy (Revised)

The GIAC Information Sensitivity Policy is a revision of the SANS Information Sensitivity Policy. The overall framework is used, as well as much of the original content, with extensive modification customized to fit GIAC's environment. For example, the data classification scheme has been redefined to add a higher level of protection for the "crown jewels". A subset "Confidential" category is included to address patient data protection, as required by HIPAA. Where the Policy statement lacks depth in subsections 3.1, 3.2, and 3.3, the revised version provides more detailed guidance in handling sensitive information. Identity verification guidelines are added to address GIAC's specific concern relative to social engineering threats. These guidelines serve as a reference on how to prevent inadvertent disclosure of protected information by the naïve employee. Some background information is added, as well as responsibility assignments for a Chief Information Officer, Information Security Officer, Managers, and all GIAC Personnel. For the full text version of the revised GIAC Enterprises Sensitivity Policy, refer to Appendix B.

Develop Security Procedures

The GIAC Information Sensitivity Policy establishes a data classification scheme and guidance for handling data or information according to its established classification level. This assignment section provides a procedure to implement the GIAC Information Sensitivity Policy. This procedure represents only one in of several procedures written to implement the GIAC Information Sensitivity Policy, establishing the methods and instructions to review Policy compliance, relevance, and effectiveness.

Procedures for Information Sensitivity Policy Compliance Review

Specific Authority
Section 6 - GIAC Enterprises Information Sensitivity Policy

1. Purpose
This procedure establishes the methods and steps for ensuring compliance with Information Sensitivity Policy, in order to verify the Policy's effectiveness and implementation throughout the company. The Information Sensitivity Policy is an enforcement strategy developed to safeguard information assets against predicted threats. The strategy dictates the technologies, resources, tactics, and training required for enforcement.[28] Reviewing compliance provides the information necessary to analyze the effectiveness of the Policy's enforcement

[28] Control Data Company. "Why Policies Fail". *White Paper*. 1999. 2 Mar. 2003. <http://downloads.securityfocus.com/library/Why_Security_Policies_Fail.pdf>

strategy. These procedures will provide indicators of the Policy's success or failure in achieving the intended goal -- to reduce the risks associated with inadvertent or unauthorized disclosure of Protected information.

2. Scope

This procedure applies to the activities established to review company-wide compliance with the GIAC Information Sensitivity Policy (reference section 6.0 of the Policy). This review procedure focuses on two major policy compliance areas: the handling of information according to its designated classification level, and employee awareness of the data classification scheme. This procedure is applicable to executive offices, divisions, departments, centers, and units.

This procedure does not cover remedial actions taken in relation to non-compliance findings, the periodic informal compliance reviews conducted by Unit Managers, or the process for revising policy and procedures based upon review findings.

3. Procedure

a. Roles and Responsibilities

Responsibility	*Action*
Information Security Officer	1. Serve as the point of contact with higher headquarters concerning violations of federal requirements, legislative mandates discovered in the compliance review process. 2. Taking into account the final BU review findings the ISO shall, prepare a final summary report for the CIO, including recommendations for any Policy areas needing revision or redefinition.
Compliance Subcommittee Leader	3. Designates an individual or team to conduct compliance reviews at within each Business Unit (BU) at all GIAC office locations. 4. Appoints CR Team Lead responsible for overall coordination of the review at each GIAC office location (multiple Business Units). 5. Develops a compliance checklist based upon either "known" weak areas, or random information handling procedures to be reviewed. The compliance checklist will be updated annually, at least 60 days prior to each BU review.

Compliance Reviewer	6. Shall be thoroughly familiar with all GIAC Security Policies, Procedures, and Standards. 7. Must not be affiliated with the unit being reviewed, nor have any authority in effecting policy or procedure decisions. 8. Conducts on-site compliance review at their designated BU once annually. 9. Coordinates pre-on-site visit requirements with the BU Managers. 10. Using scenarios, quiz BU employee's knowledge of data classification scheme. Notes observations and comments. 11. Using Compliance Checklist as a guideline, observe or question BU employees about information sensitivity handling policies and procedures. 12. Completes and submits to the BU Manager, CSL, and ISO the Field Compliance Review Report. 13. Completes and submits to the CSL and ISO Summary of Recommendations and BU Management Response.
Business Unit Manager	14. Responsible for ensuring that subordinate employees complete the exam within 90 days of the on-site visit compliance review. 15. Forwards test results to their designated CR within 30 days of the on-site visit.
GIAC Employee	16. Participate in bi-annual training and testing to ensure understanding of data classification scheme and policy awareness. 17. Participates, if asked questions or asked to demonstrate a particular task by the CR during on-site review.

b. Compliance Review Process

1. Each Business Unit will be subject to a compliance review no less than once per calendar year.

2. The Compliance Review process shall be based upon approved standards and guidelines set forth in the GIAC Information Sensitivity Policy framework, and shall include the following:

(a.)Employee Awareness Assessment *(This step helps to measure the individual employee's awareness of data classification and information handling standards set forth in the Policy).*

i. The Information Sensitivity Awareness test is a web-based exam, accessible via the GEIS portal (see Figure 2). Exam IDs and passwords shall be issued to subordinates by the BU Manager to ensures that subordinates are grouped according to the appropriate BU.
ii. BU Managers are responsible for ensuring that subordinate employees complete the exam within 90 days of the Compliance Review.
iii. BU Managers will forward test results to their designated CR within 30 days of the on-site visit.
iv. The CR will review collective BU results with the BU manager

during the on-site visit, providing BU managers the opportunity to enter remarks in the CR's review findings report.

v. Online exam results are not included as a finding in the CR's review report, as they are electronically forwarded to the CSL and ISO at the time of submission for incorporation into the ISO's report summary to the CIO.

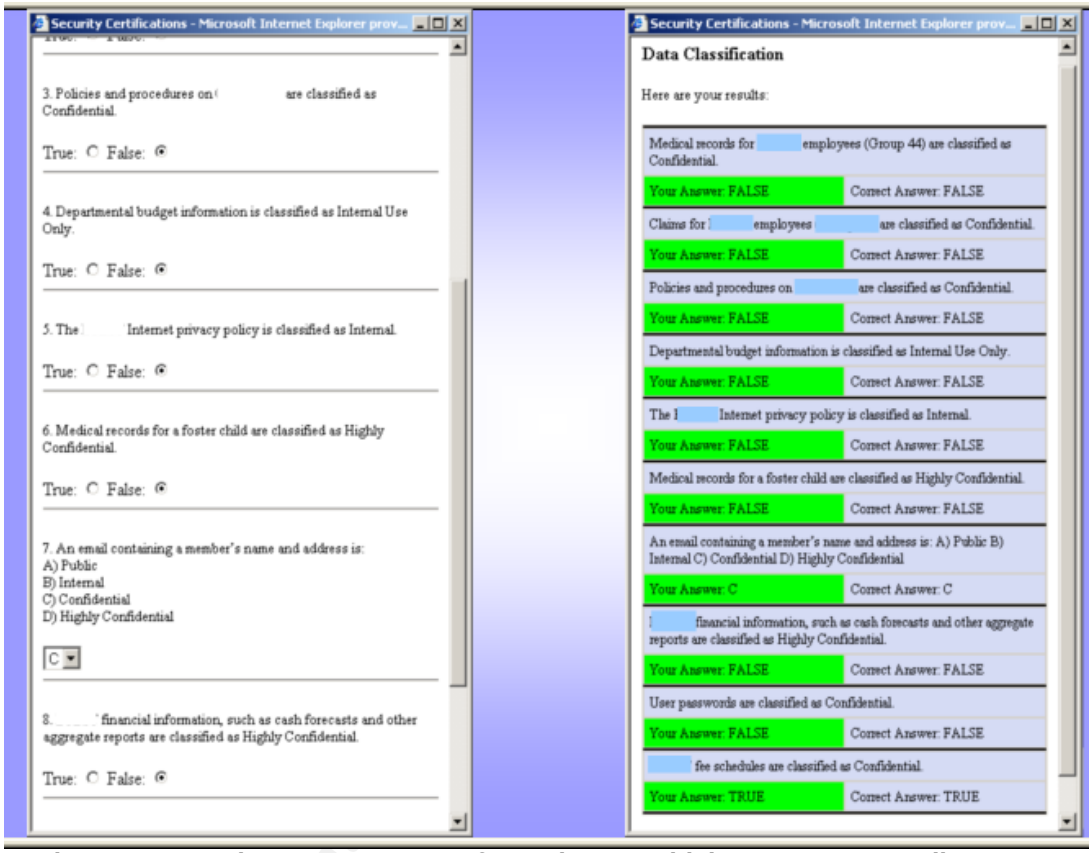

Figure 2 - Sample Screen - GEIS Information Sensitivity Awareness Online Exam
(Actual screenshot source: Iris Security Awareness Portal Online Demonstration)[29]

(b.) On-site Visit. The CR's on-site review will assess the BU's compliance with the Information Sensitivity Policies and Standards, and shall include the steps as described below.

i. Using the Compliance Checklist as a guide, the CR will inspect the BU's facilities and equipment;
ii. Interview the BU's operations and management personnel, and
iii. Review all other necessary documents and data as considered necessary.

(c.) Review Findings. The CR's findings will be documented in a report that will

[29] Itillious, Inc. Screenshot source: Iris Security Awareness Portal Online Demonstration

include at least the following elements:

i. The scope of the review, (*list of standards being reviewed- based upon compliance checklist*)
ii. Findings; *(based on the BU's compliance with the Information Sensitivity Policies and Standards. All findings of non-compliance will be clearly described)*
iii. The reviewed BU's response to the review report findings; (*includes a statement as to whether they agree or disagree with the finding(s). If they agree, the report should also include the date they will provide a detailed mitigation plan that corrects the areas on non-compliance. If they disagree, the audit report should include their detailed clear description why they disagree.)*

(d). Communication of Findings

i. Review Findings and Management Comments: This form shall be used a guideline for documenting the audit findings, recommendations for improvement and comments from management representatives. This form, along with the Summary of Recommendations & Management Response Form are intended to be incorporated into the CR's final report.

Review Findings and BU Management Comments Form

Review Test Results	***Possible Risk Exposure***	***BU Management Comments***	***Report Item***	
			Procedural	***Best Practice***
Finding: ***Recommendation:***				

ii. The CR is responsible for developing a draft review report and presenting it to the BU being auditing for their review and written response. As appropriate, any differences of opinion on the review results should be discussed to ensure both entities clearly understand each other's position.
iii. The draft report with the BU responses shall be sent to the Compliance Subcommittee within two (2) weeks following the on-site visit, and distributed to the reviewed BU for review and a written response.
iv. Within 30 days of receipt of the report, the BU being reviewed is required to submit a written response on any issues raised or recommendations made in the reviewed report.
v. The CSL shall ensure that follow-up reviews are conducted to assess action taken on the specific recommendations made in previously issued reports.

vi. Summary of Recommendations & Management Response: This form summarizes the recommendations generated by the review and the actions agreed to be taken by the BU Manager to address the review issues.

Summary of Recommendations & Management Response Form

Recommendations	Procedural	Best Practice	Management Response		
			Disagree	Agree	Action Taken

i. The CR shall issue a written report to the BU and Compliance Subcommittee, with copies to other officials as appropriate, at the conclusion of each review assignment. The CIO and ISO shall be provided with a copy of all such reports.

(e). Follow-up and Corrective Actions.

i. The review does not cease with the issuance of the results. It should be determined whether responsible parties actually correct the deficiencies noted in the review and implement all of the recommended corrective actions in a timely and accurate manner.

ii. The CSL shall ensure that follow-up reviews are conducted to assess action taken on the specific recommendations made in previously issued reports.

References

18 U.S.C. 90 "Economic Espionage Act §§ 1831-1839". 12 Jan. 2003 <http://www.tscm.com/USC18_90.html>

"2002 Computer Crime and Security Survey". *Internet Psychology Research Institute (IPRI) Home Page.* 19 Jan. 2003. <http://www.internet-psychology.org/efraud/computer-crime.htm>

Best Practices, LLC. "Sample Report Summary: Pharma Technical Services: Structuring for Manufacturing Process Ownership." 12 Jan. 2003. <http://www.benchmarkingreports.com/businessoperations> /op84_technical_services.asp>

Black, Henry C. Black's Law Dictionary. 6th ed. New York: West Group, 1990.

Business Wire. "Leading Pharmaceutical Companies Use Ensure's Innovative Security To Protect Intellectual Property, Meet Information Security Regulations." *Pharmaceutical Online Home Page.* 23 Sep. 2002. 11 Jan. 2003. <http://www.pharmaceuticalonline.com/content/news/>

Chapple, Mike, Deborah Shinder, and Ed Tittle. "TICSA Certification: Information Security Basics." *InformIT.com* 22 Nov. 2002. 18 Jan. 2003. <http://www.informit.com/isapi/product_id~%7BE9081702-D789-4795-B7DE-6315866D67CC%7D/element_id~%7B4C230C18-7506-49E7-95F9-A0F00C7A7F1E%7D/st~%7B5947591F-62F3-4B59-B9CC-35BAC4E3C229%7D/content/articlex.asp>

"Cisco PIX 500 Series Firewalls". *Cisco, Inc. Home Page.* 2002. 3 Mar. 2003. http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/

Control Data Company. "Why Policies Fail". *White Paper*. 1999. 2 Mar. 2003. <http://downloads.securityfocus.com/library/Why_Security_Policies_Fail.pdf>

"Dispersed and Global Project Teams." *groupvision Switzerland Home Page.* <http://www.groupvision.ch/services/text/2-imeetings.htm >

"ERA Commons". *Computer Retrieval of Information on Scientific Projects (CRISP) Home Page*. 18 Jan. 2003. <http://crisp.cit.nih.gov/>

Erwin, Dan. "e-risk, Liabilities in a Wired World." *Computer Security Alert Home Page*. Aug. 2000. 17 Jan. 2003. <http://www.gocsi.com/pdfs/erisk.pdf>

"FASP Areas". 27 Dec. 2002. 18 Jan. 2003. <http://csrc.nist.gov/fasp/ FASPDocs/risk-mgmt/system-sensitivity.doc>

Fenwick and West LLP. Home Page. Trade Secrets Group. 2002. 16 Jan. 2003. <http://www.fenwick.com/About_Fenwick/ip/trade_secrets /Trade_Secrets_Group.htm>.

Gibaldi, Joseph. MLA Handbook for Writers of Research Papers. 5th ed. New York: Modern Language Association of America, 1999.

Harnack, Andrew and Kleppinger, Eugene. “Using Principles of MLA Style to Cite Internet Sources.” *Online! A Guide to Using Internet Sources*. 17 Jan 2003. <http://www.bedfordstmartins.com/online/cite5.html>

Harris, Shon. CISSP All-in-One Certification Exam Guide. California: McGraw-Hill/Osborne, 2002.

“HIPAA & Research Recruitment Alternatives.” 18 Jan. 2003. <http://www.mwri.magee.edu/hipaa/alternatives.pdf>

Itlillious, Inc. Home Page. “Iris n. Itlillious’ Security Awareness Portal” 3 Mar 2003. <http://www.itillious.com/iris/dataclass.html>

Johnson, Kevin. “Security of Pharmaceutical Intellectual Property in the Era of Electronic Regulatory Submissions.” 2000. 17 Jan 2003. <http://www.pharmaknowledge.com/Security%20-%20KJohnson%20presentation.pdf>

Kettler, Hannah. “Updating the Cost of a New Chemical Entity.” 11 Dec 2002. 17 Jan 2003. <http://www.ohe.org/updating.htm>

Marquart, Christopher. “The Computer Security Professional’s Role in Trade Secret Protection” <http://csrc.nist.gov/nissc/1999/proceeding/papers/t18.pdf>.

Miller, Steven. “Competitive Intelligence – An Overview”. *Competitive Intelligence Magazine*. <http://www.scip.org/Library/overview.pdf>.

Mitnick, Kevin D. and Simon, William L. The Art of Deception. Indiana: Wiley Publishing, 2002.

Perseid Software Limited. “Building Mission Critical Document Management Solutions for Global Pharmaceutical Companies”. May 2001. *EMC Home Page.* 15 Jan. 2003 <http://www.emc.com/vertical/pdfs/life_sciences/EMC_GMPwpFinal1.pdf>

Perseid Software Limited. “Creating a Global IT Infrastructure for Clinical Trials”. *EMC Home Page.* Oct. 2001. 17 Jan 2003 <http://www.emc.com/vertical/pdfs/life_sciences/EMC_clinical_trials.pdf>

Plumtree Software Home Page. 17 Jan. 2003. <http://www.plumtree.com/customers/industries/pharmaceuticals_healthcare/pharmacia.asp>.

Plumtree Software Home Page. “RSA ClearTrust Ready Implementation Guide For Portal Servers and Web-Based Applications”. 13 Nov. 2002. 18 Feb. 2003. <http://rsasecurity.agora.com/rsasecured/guides/cleartrust/Plumtree_Corporate_Portal_v4_5_CT50.pdf>

PricewaterhouseCoopers. Pharmaceutical Regulatory and Compliance Congress and Best Practices Forum. *Pharmaceutical Compliance Forum Online.* 15 Nov. 2002. 11 Jan. 2003. <http://www.pharmacongress.com/overview.html>

Rx2000 Institute Home Page. “Health Insurance Portability and Accountability

Act (HIPAA) Frequently Asked Questions." 16 Jan. 2003. URL: http://www.rx2000.org/KnowledgeCenter/hipaa/hipfaq.htm#Intro

Schneider, Ilene. "Meeting the Mandate: Pharmaceutical companies team with vendors and gear up to comply with 21 CFR Part 11". 5 Mar. 2001. 15 Jan. 2003. <http://www.dddmag.com/feats/0102regs.asp>

Swiatocha, Michael. "Conducting a Clinical Compliance Risk Assessment in the Pharmaceutical Industry". 25 Mar. 2002. 11 Jan. 2003. <http://www.ehcca.com/presentations/ressummit2/3_03.pdf>

The Society of Competitive Intelligence Professionals (SCIP) Home Page. 18 Jan. 2003. <http://www.scip.org/index.asp>

U.S. Food and Drug Administration (FDA) Home Page. "Current Good Manufacturing Practice (CGMP) Regulations: Division of Manufacturing and Product Quality (HFD-320)." 9 Jan. 2003. Center for Drug Evaluation and Research. 13 Jan 2003. <http://www.fda.gov/cder/dmpq/>

Weil Gall, Barbara. "An Overview of Intellectual Property Protection." *GigaLaw.com.* Oct. 2000. 19 Jan. 2003 **<**http://www.gigalaw.com/articles/2000-all/gall-2000-10-all.html>

"What Are the Lessons of Eli Lilly's FTC Settlement In Major Breach of Patient Privacy?" *Managed Care Week.* 4 Feb 2002. 17 Jan 2003. <http://www.rxsolutions.com/c/pbi/pbi_view.asp?docid=131>

WindowsSecurity.com Home Page. "Internet Security Policy – Risk Profiling". 16 Oct. 2002. 3 Mar. 2003. <http://secinf.net/policy_and_standards/Internet_Security_Policy/Internet_Security_Policy__Risk_Profiling.html>

Appendix A: Model Information Sensitivity Policy

*(**NOTE:** This Information Sensitivity policy was obtained from The SANS Institute's Security Policies Project at URL: http://www.sans.org/resources/policies/Information_Sensitivity_Policy.doc. The original verbiage of this model is not modified in this section.)*

1.0 Purpose

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of <Company Name> without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect <Company Name> Confidential information (e.g., <Company Name> Confidential information should not be left unattended in conference rooms).

Please Note: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to Infosec.

2.0 Scope

All <Company Name> information is categorized into two main classifications:

- <Company Name> Public
- <Company Name> Confidential

<Company Name> Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to <Company Name> Systems, Inc.

<Company Name> Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to the success of our company. Also included in <Company Name> Confidential is information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of <Company Name> Confidential information is "<Company Name> Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to <Company Name> by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into <Company Name>'s network to support our operations.

<Company Name> personnel are encouraged to use common sense judgment in securing <Company Name> Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager

3.0 **Policy**

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as <Company Name> Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the <Company Name> Confidential information in question.

3.1 **Minimal Sensitivity:** General corporate information; some personnel and technical information.

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "<Company Name> Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "<Company Name> Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, <Company Name>

information is presumed to be "<Company Name> Confidential" unless expressly determined to be <Company Name> Public information by a <Company Name> employee with authority to do so.

Access: <Company Name> employees, contractors, people with a business need to know.

Distribution within <Company Name>: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of <Company Name> internal mail: U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.

Electronic distribution: No restrictions except that it be sent to only approved recipients.

Storage: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.

Disposal/Destruction: Deposit outdated paper information in specially marked disposal bins on <Company Name> premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

3.2 **More Sensitive:** Business, financial, technical, and most personnel information

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". As the sensitivity level of the information increases, you may, in addition or instead of marking the information "<Company Name> Confidential" or "<Company Name> Proprietary", wish to label the information "<Company Name> Internal Use Only" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.

Access: <Company Name> employees and non-employees with signed non-disclosure agreements who have a business need to know.

Distribution within <Company Name>: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of <Company Name> internal mail: Sent via U.S. mail or approved private carriers.

Electronic distribution: No restrictions to approved recipients within <Company Name>, but should be encrypted or sent via a private link to approved recipients outside of <Company Name> premises.

Storage: Individual access controls are highly recommended for electronic information.

Disposal/Destruction: In specially marked disposal bins on <Company Name> premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

3.3 **Most Sensitive:** Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that <Company Name> Confidential information is very sensitive, you may should label the information "<Company Name> Internal: Registered and Restricted", "<Company Name> Eyes Only", "<Company Name> Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of <Company Name> Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.

Access: Only those individuals (<Company Name> employees and non-employees) designated with approved access and signed non-disclosure agreements.

Distribution within <Company Name>: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.

Distribution outside of <Company Name> internal mail: Delivered direct; signature required; approved private carriers.

Electronic distribution: No restrictions to approved recipients within <Company Name>, but it is highly recommended that all information be strongly encrypted.

Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.

Disposal/Destruction: Strongly Encouraged: In specially marked disposal bins on <Company Name> premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

4.0 **Enforcement**

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

5.0 Definitions

Terms and Definitions

Appropriate measures. To minimize risk to <Company Name> from an outside business connection. <Company Name> computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access <Company Name> corporate information, the amount of information at risk is minimized.

Configuration of <Company Name>-to-other business connections. Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

Delivered Direct; Signature Required. Do not leave in interoffice mail slot, call the mail room for special pick-up of mail.

Approved Electronic File Transmission Methods. Includes supported FTP clients and Web browsers.

Envelopes Stamped Confidential. You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.

Approved Electronic Mail. Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, [insert corporate supported mailers here…]. If you have a business need to use other mailers contact the appropriate support organization.

Approved Encrypted email and files. Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within <Company Name> is done via a license. Please contact the appropriate support organization if you require a license.

Company Information System Resources. Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.

Expunge. To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data, supplied as a part of Norton Utilities. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten. The same thing happens on UNIX machines, but data is much more difficult to retrieve on UNIX systems.

Individual Access Controls. Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the chmod command (use *man chmod* to find out more about it). On Mac's and PC's, this includes using passwords on screensavers, such as Disklock.

Insecure Internet Links. Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of <Company Name>.

Encryption. Secure <Company Name> Sensitive information in accordance with the *Acceptable Encryption Policy*. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

One Time Password Authentication. One Time Password Authentication on Internet connections is accomplished by using a one time password token to connect to <Company Name>'s internal network over the Internet. Contact your support organization for more information on how to set this up.

Physical Security. Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer

cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Private Link. A Private Link is an electronic communications path that <Company Name> has control over its entire distance. For example, all <Company Name> networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer have established a private link. ISDN lines to employee's homes is a private link. <Company Name> also has established private links to other companies, so that all email correspondence can be sent in a more secure manner. Companies which <Company Name> has established private links include all announced acquisitions and some short-term temporary links

6.0 Revision History

Appendix B: GIAC Information Sensitivity and Protection Policy (Revised)

Background

GIAC Enterprises generates, receives and stores volumes of information of a sensitive nature. Some consist of GIAC trade secrets (i.e. chemical compound formulas) that are key to the company's profitability, competitiveness, and possibly its survivability. Other information contains Privileged data that GIAC is morally, ethically, and legally responsible for protecting. Some information, though seemingly "harmless", provide information may be used by a social engineer to piece together the structure of the company, provide clues about what kind of computer systems we use, and most importantly, obtain the names, titles, and telephone numbers of GIAC employees. The greatest harm resulting from disclosing sensitive information comes from the actions of individuals, both intentional and unintentional. Only by defining information sensitivity levels and providing guidelines for handling information according to their classification or sensitivity levels, can GIAC begin to minimize disclosure risks.

1. Purpose

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of GIAC Enterprises without proper authorization. The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect sensitive material (e.g., Protected information should not be left unattended in conference rooms).

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to the GIAC Information Security Officer (ISO).

2. Scope

All GIAC information is categorized into four main classifications: *Sensitive*, *Confidential, Private*, and *Public*. These classifications are defined as follows:

**** Note:*** *"Protected" information refers to any data categorized or classified as Sensitive, Confidential, or Private.*

SENSITIVE: This classification applies to information that requires special precautions to assure the integrity of the information, by protecting it from unauthorized modification or deletion. It is information that requires a higher than normal assurance of accuracy and completeness. Examples of sensitive information include GIAC trade secrets, financial transactions, regulatory actions, development programs, potential acquisition targets, and other information integral to the success of our company.[30]

CONFIDENTIAL: This classification applies to the most sensitive business information that is intended strictly for use within GIAC. This information is exempt from disclosure under the provisions of the Freedom of Information Act or other applicable federal laws or regulations. Its unauthorized disclosure could seriously and adversely impact GIAC, its stockholders, its business partners, and/or its customers. Health care-related information should be considered at least CONFIDENTIAL.

There are two subsets of CONFIDENTIAL information: *Third Party Confidential* and *Privileged Confidential*.

Privileged Confidential is information that is protected from disclosure pursuant to the rules of privilege recognized by law. Examples of this type of information are personally identifiable health data that GIAC is not only ethically and morally responsible to protect, but also bound to protect by legislative mandate (e.g. patient data used clinical trial research).

Third Party Confidential contains information belonging or pertaining to another corporation that has been entrusted to GIAC by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into GIAC's network to support our operations.

PRIVATE: This classification applies to personal information that is intended for use within GIAC. Its unauthorized disclosure could seriously and adversely impact GIAC and/or its employees. Included is information that is less critical, such as telephone directories, general corporate information, personnel information, etc., which does not require as stringent a degree of protection.

PUBLIC: This classification applies to information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to GIAC Enterprises.

GIAC personnel are encouraged to use common sense judgment in securing all levels of information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their

[30] WindowsSecurity.com Home Page. "Internet Security Policy – Risk Profiling". 16 Oct. 2002. 3 Mar. 2003. <http://secinf.net/policy_and_standards/Internet_Security_Policy/Internet_Security_Policy__Risk_Profiling.html>

manager or the GIAC.

3. Roles and Responsibilities.

A. Chief Information Officer

The Chief Information Officer (CIO) is responsible for establishing and implementing security policies and procedures, and for initiating and supervising measures needed to ensure compliance with security regulations. The CIO shall:

1. Serve as the point of contact with higher headquarters concerning security matters.
2. Ensure that the policy is compliant with federal audit requirements and other legislative mandates.
3. Ensure visibility and management support for the Information Sensitivity policy.
4. Determine the data classification scheme.
5. Determine the security access requirements for all positions.
6. Investigating formal inquiries into reports of Policy violations based upon ISO's preliminary review.

B. Information Security Officer (ISO)

The Information Security Officer (ISO) is responsible for the following:

1. Establishing procedures and monitoring their implementation for safeguarding Protected information.
2. Recommending procedures for ensuring that all personnel who are to handle Protected information are appropriately cleared and trained in information security procedures.
3. Reviewing preliminary and formal inquiries into reports of Policy violations.
4. Defining procedures to implement the policy;
5. Ensuring that the policies are put into effect; related technical solutions are deployed;
6. Ensuring that users receive information and training about the policy and related procedures;
7. Ensuring that user testing is conducted bi-annually to ensure understanding of data classification scheme and policy awareness;
8. Ensuring all personnel are trained in the computer security responsibilities and duties associated with their jobs;
9. Ensuring that the policy is enforced, and that violators are punished as prescribed by policy;
10. Executing a program of document review to reduce unneeded classified holdings, consistent with operational requirements;
11. Ensuring that the policy is reviewed at least once annually for continued relevance and accuracy;

12. Ensuring that policy is revised once annually as needed to remain current, relevant, and accurate; and,
13. Ensuring participation by all levels of management and administrative and technical staff during planning, development, and implementation of policy and procedures.

C. General Management Responsibility

Managers are responsible for security of sensitive information within their departments. By assuring that personnel comply with this Policy, managers will provide the control necessary to protect the confidentiality of the protected information.

Managers at all levels are responsible for:

1. Identifying positions under their supervision that require special trust. (Applicants for and incumbents in those positions must be screened, trained, and managed in ways that will ensure an adequate level of security for sensitive information to which they have access.)
2. Briefing each subordinate on security requirements and procedures as part of the normal orientation procedures.
3. Monitor adherence the information sensitivity requirements outlined in this policy.
4. Persons having access to protected data are properly cleared and that employee conduct is monitored, as required by appropriate security regulations.
5. Procedures are followed for the handling of protected data.
6. In addition, supervisors are responsible for reporting violations of security procedures, or practices dangerous to security, to the appropriate security personnel.
7. Ensuring that all personnel are trained in the data handling responsibilities and duties associated with their jobs.
8. Informing GIAC ISO when user access is to be removed.

D. GIAC Personnel

All GIAC personnel (including employees, contractors and temporary employees) shall understand their responsibilities and duties to protect information at levels of classification as prescribed by this policy. When dealing with Protected information, all GIAC personnel shall:

- not permit unauthorized access to their account;
- not share account login userID and password with others;
- limit printing and reproduction of certain Protected material;
- use key and encrypted computer data access to control theft of secret computer-stored information;
- not attempt to access information for which they have not been given authorization;
- use proper handling procedures for Protected printed

information;
- understand the consequences of their failure to adhere to statutes and policy governing information resources; and,
- immediately notify supervisor of suspected misuse of data, security breach, or other violations of this policy.

All personnel with access to Protected information are responsible for being knowledgeable of all applicable regulations concerning the safeguarding of the information, material, or equipment.

4. Policy

The Data Handling Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines serve as a reference only, as the examples in each subsection may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of Protected Data information in question.

A. Sensitive Data:

	Sensitive Classification Handling Guideline
**** Identity Verification:***	Verify identity of requester as active employee or verify non-disclosure agreement on file and management approval for non-GIAC personnel.[31]

** Information verification guidelines address GIAC's specific concern relative to social engineering threats. These guidelines serve as a reference on how to prevent inadvertent disclosure of protected information.*

Access:	Only those individuals (GIAC employees and non-employees) designated with approved access and signed confidentiality and non-disclosure agreements.
Distribution within GIAC:	Delivered direct - signature required, envelopes stamped Senistive, or approved electronic file transmission methods.
Distribution outside of GIAC internal mail:	Must be distributed via approved private carriers or delivered directly. Signature is required.
Electronic distribution:	No restrictions to approved recipients within GIAC, but it is highly recommended that all information be strongly encrypted. Sensitive information must not be sent by email, except by approval of the ISO. If email transmission is authorized, the message must be encrypted, so that it is only readable by the intended recipient using GIAC-approved software and algorithms.
Marking in hardcopy or electronic form:	Marking guidelines for information in hardcopy or electronic form. Note: any of these markings may be used with the additional annotation of "3rd Party Confidential" or "Privileged Confidential". To indicate that GIAC Confidential information is very sensitive, you

[31] Mitnick, Kevin D. and Simon, William L. The Art of Deception. Indiana: Wiley Publishing, 2002. p. 336.

	may should label the information "GIAC Internal: Registered and Restricted", "GIAC Eyes Only", "GIAC Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of GIAC Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.
Storage:	Individual access controls are very highly recommended for electronic information. Physical security is used, and information should be stored in a physically secured computer. File Protected documents in locked files, apart from non-Protected material. Remote users should not maintain Protected information on their systems unless adequately secured via encryption or authenticated access control mechanisms. This is especially important if the system is also used to connect to the Internet.
Disposal/Destruction:	Hardcopy: In specially marked disposal bins on GIAC premises; GIAC Confidential documents containing trade secret data shall be also be cross-cut, re-shredded and mixed to ensure that information cannot be reconstructed and read. No recycling bins allowed. Softcopy: Expunged/cleared. Reliably erase or physically destroy media.

B. Confidential Data: (Including sub-categories "Third-party and Privileged Confidential)

	Confidential Classification Handling Guideline
Identity Verification:	Verify identity of requester as active employee or non-GIAC employee with authorization. Check with human resources department to disclose Confidential information to authorized employees or external requesters.[32]
Access:	GIAC personnel (employees and non-employees) with signed non-disclosure agreements who have a business need to know.
Distribution within GIAC:	May distribute via standard interoffice mail with appropriate marking on external envelope, approved electronic mail and electronic file transmission methods.
Distribution outside of GIAC internal mail:	May be distributed via U.S. mail and other public or private carriers. May be distributed via approved electronic mail and electronic file transmission methods but must be encrypted.
Electronic distribution:	No restrictions to approved recipients within GIAC, but should be encrypted or sent via a private link to approved recipients outside of GIAC premises.
Marking in hardcopy or electronic form:	Note: any of these markings may be used with the additional annotation of "3rd Party Confidential" or "Privileged Confidential". As the sensitivity level of the information increases, you may, in addition or instead of marking the information "GIAC Confidential" or "GIAC Proprietary", wish to label the information "GIAC Internal Use Only" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.

[32] Mitnick, Kevin. p. 336.

Storage:	Individual access controls are highly recommended for electronic information. Individual access controls are very highly recommended for electronic information. File Protected documents in locked files, apart from non-Protected material. Remote users should not maintain Protected information on their systems unless adequately secured via encryption or authenticated access control mechanisms. This is especially important if the system is also used to connect to the Internet.
Disposal/Destruction:	In specially marked disposal bins on GIAC premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

C. Private Data:

	Private Classification Handling Guideline
Identity Verification:	Verify identity of requester as active employee or verify non-disclosure agreement on file and management approval for non-GIAC personnel. [33]
Access:	GIAC personnel (employees, contractors, temporary employees) -- people with a business need to know.
Distribution within GIAC:	May be distributed internally in any form, including interoffice mail, internal email.
Distribution outside of GIAC internal mail:	May be distributed via U.S. mail and other public or private carriers. May be distributed via approved electronic mail and electronic file transmission methods but must be encrypted.
Electronic distribution:	No restrictions except that it is sent only to approved recipients.
Marking in hardcopy or electronic form:	Note: any of these markings may be used with the additional annotation of "3rd Party Confidential" or “Privileged Confidential”. Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "GIAC Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "GIAC Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no marking is present, GIAC information is presumed to be "GIAC Confidential" unless expressly determined to be Public information by personnel with authority to do so.
Storage:	Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate. Individual access controls are recommended for electronic information where needed. File Protected documents in locked files, apart from non-Protected material.
Disposal/Destruction:	Deposit outdated paper information in specially marked disposal bins on GIAC premises; electronic data should be

[33] Mitnick, Kevin. P. 335.

expunged/cleared. Reliably erase or physically destroy media.

5. Enforcement and Penalty for Deliberate or Inadvertent Disclosure of Protected Data.

Unauthorized personnel are not allowed to see or obtain Protected Data. The gross negligence or willful disclosure of Protected Data documents can result in prosecution for misdemeanor or felony resulting in fines, imprisonment, civil liability, and/or dismissal.

6. Compliance Reviews

It is critical to ensure that this Policy is being consistently applied throughout the company. Without auditing or reviewing how and to what extent it is implemented, this Policy is useless. Reviews should be conducted by a GIAC employee that has no authority to effect policy and procedural decisions.

The review process should be based upon this Policy framework and should include the following:

1. Individual employee awareness testing – This should be occur bi-annually, using an internal web-based test, accessible via the GEIS portal. The Compliance Subcommittee will collect and assess the results.
2. An internal auditor should be designated for each GIAC office location. For large locations, two auditors may be assigned. The internal auditor should monitor compliance with this Policy checking against selected compliance matrix procedures established by the ISO. This process should occur annually.

Unit managers or designated security managers should also conduct unannounced spot checks of Protected information handling procedure compliance within their units.

7. Maintenance and Revision

The ISO is responsible for maintaining this policy and ensuring compliance. The Information Sensitivity Policy will be reviewed and revised annually by the CIO and its appointed committee.

8. Terms and Definitions

Appropriate measures: To minimize risk to GIAC from an outside business connection. GIAC computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access GIAC corporate information, the amount of information at risk is minimized.

Configuration of GIAC-to-other business connections: Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

Delivered Direct; Signature Required: Do not leave in interoffice mail slot, call the mail room for special pick-up of mail.

Approved Electronic File Transmission Methods: Includes supported FTP clients and Web browsers.

Envelopes, Stamped "Confidential": You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.

Approved Electronic Mail: Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, [insert corporate supported mailers here…]. If you have a business need to use other mailers contact the appropriate support organization.

Approved Encrypted email and files: Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within GIAC is done via a license. Please contact the site IT Support Team if you require a license.

Company Information System Resources: Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.

Expunge: To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data, supplied as a part of Norton Utilities. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten. The same thing happens on UNIX machines, but data is much more difficult to retrieve on UNIX systems.

Individual Access Controls: Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the chmod command (use *man chmod* to find out more about it). On Mac's and PC's, this includes using passwords on screensavers, such as Disklock.

Insecure Internet Links: Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of GIAC.

Encryption: Secure GIAC Sensitive information in accordance with the *Acceptable Encryption Policy*. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

One Time Password Authentication: One Time Password Authentication on Internet connections is accomplished by using a SecureID one-time password token to connect to GIAC's internal network over the Internet.

Physical Security: Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Privileged Confidential Data: Data that is protected from disclosure pursuant to the rules of privilege recognized by law, i.e. individually identifiable health information as prescribed by HIPAA.

Private Link: An electronic communications path that GIAC has control over its entire distance. For example, all GIAC networks are connected via a private link. A computer with modem connected via a standard “land line” (not cell phone) to another computer has established a private link. ISDN lines to employee's home is a private link. GIAC also has established private links to other companies, so that all email correspondence can be sent in a more secure manner. Companies that GIAC has established private links include all announced acquisitions and some short-term temporary links

Trade Secrets: Information including, but not limited to, technical or non-technical data, a formula, a pattern, a compilation, a program, a device, a method, a technique, a drawing, a process, financial data, financial plans, product plans, or a list of actual or potential customers or suppliers which (i) derives economic value, actual or potential, from not being generally known to and not being readily ascertainable by proper means by other persons, who can obtain economic value from its disclosure or use; and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

7.0 Revision History

Initial Revision 1.0, on January 23, 2003 by Janis Orsino