Global Information Assurance Certification Paper

GIAC – ISO Certification Program:

Practical Assignment - Version 1.2

Submitted by:
Paul Jennings
May 6, 2002

"GIAC Health Enterprises: Medical Record Security in Transition"

Table of Contents

Introduction

Established in 1955, GIAC Health Enterprises (GIAC-HE) is a privately owned, for-profit, multi-specialty medical group. GIAC-HE is currently staffed by 45 physicians (MD's), 20 physician assistant/nurse practitioners, and approximately 240 clinical and operations staff. Medical and surgical specialties are represented. Medical and ancillary (laboratory, radiology, cardio-pulmonary) services are rendered from one primary campus and 2 satellite offices located within a fifteen mile radius.

GIAC-HE IT Infrastructure

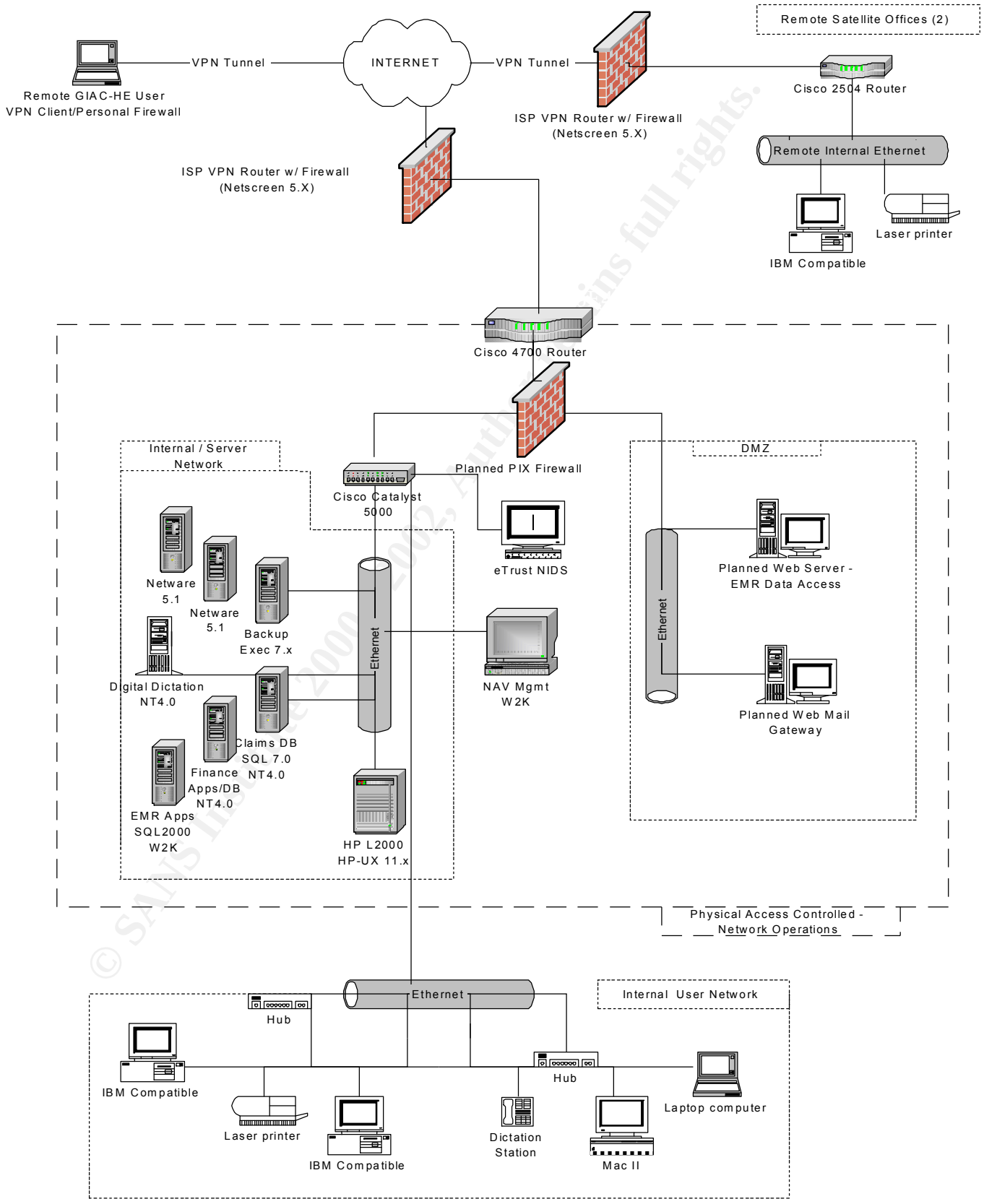
GIAC-HE's network, originally implemented in 1996, has successfully met the objectives of establishing an infrastructure intended to support continuing growth and diversity of services provided. A 1996 IT strategic plan identified the implementation of an electronic medical record as the five to seven year goal. Additionally, intermediate goals to provide network-based applications and services have not required significant changes to the infrastructure, beyond adding server, storage, and backup capabilities. GIAC-HE has standardized its network hardware, using Compaq servers (and one HP-L2000), Cisco routers, 3Com interface cards, one multi-layer switch (Catalyst 5000), and HP switching hubs. There are five (5) local area network intermediate distribution "hub" closets (all secure behind locked doors), utilizing multi-mode 24-strand fiber optic cable for connection to the Catalyst 5000. Category 5 UTP cabling was installed throughout the facility for PC and print-server connections. This architecture allowed GIAC-HE to lower its initial network acquisition costs while providing for future growth and flexibility.

In anticipation of Internet-based access for patients to personal health care information and on-line interaction with GIAC-HE physicians, point-to-point T1 lines to satellite offices have recently been replaced with Internet-based, VPN-secured links. GIAC-HE is working closely with its Internet service provider to ensure the security and stability of these links, creating a multi-layered defense that includes Netscreen routers/firewalls and GIAC-HE based Cisco routers configured with NAT (network address translation), egress rate-limiting, and restrictive port filtering.

An eTrust "SessionWall" network-based intrusion detection system was added in 1999, shortly after network access to the Internet was implemented. This was done primarily to provide "surfing" monitoring and virus detection for Internet e-mail. As web-based access into GIAC-HE's Internet services gets closer, much more attention to the rules and actions database of this NIDS will be required to provide appropriate detection of threats that may get past the ISP's firewall and GIAC-HE's router.

Network Components

Type	Description	OS	Services
Routers (3)	Cisco4700(1), 2504 (2)	IOS 12.x	NAT, port filtering, ACL's
VPN Appl	Netscreen 5XP (ISP vendor supplied)		VPN (3DES), traffic mgmt, firewall options
Multi-Layer Switch	Cisco Catalyst 5000	IOS 3.2(8)	Ethernet, Fast Ethernet, (ATM-backplane)
IDS	CA eTrust IDS 1.4.5	NT4.0	Network-based intrusion/attack detection, email virus scanning, URL filtering, reporting and alerts
AV Mgmt	Compaq / Intel	W2K	Norton Anti-Virus Corporate Ed 7.x, Live Update Mgmt, Alert Console, Symantec Mgmt System
Servers (3)	Compaq / Intel	Netware 5.1	File, print, backup, user network authentication
Servers (3)	Compaq / Intel	NT4.0 (sp6a) MS-SQL 7.0	Claims editing, finance, HR, time & attendance, payroll, digital dictation, backup, DHCP, WINS
Server	Compaq / Intel	W2K Server MS-SQL 2K	EMR application and database, backup
Server	HP L2000 / PA-RISC	HP-UX 11.0	Group practice apps and database, backups
Server (planned)	Compaq / Intel	W2K Server MS-SQL 2K	EMR data repository web server (public only), Tripwire
Server (planned)	Compaq / Intel	W2K Server	SMTP mail gateway
Firewall (planned)	Cisco – PIX family	Tbd	Port and address filtering, RFC 2827, session mgmt, outgoing traffic limits (Convery, p.95)



Paul Jennings Practical Ver 1.2

GIAC-HE Business Operations

GIAC-HE is in the business of providing health care, and operations are structured around the following key characteristics of delivering quality medical care:

A. Accurate and timely collection of patient-specific information (demographic and health status) from the patient or guardian.
B. Complete, verifiable creation and updating of a patient's medical record (MR) as health care is delivered by multiple providers and ancillary departments, and access to the MR for ongoing care and quality assurance (peer review).
C. Creation, submission and collection of claims/bills for payment of health care services rendered.
D. Non-clinical operations required to support delivery of health care, including Accounting and Finance, Human Resources, Physician Recruitment, Facilities and Supply, Information Services (IT), and Business Administration (contracts, legal, marketing, etc.).
E. Understanding, implementing, and compliance with regulations related to the above activities, especially and most recently, HIPAA (Health Insurance Portability and Accountability Act).

A. New patients to GIAC-HE are asked to provide complete demographic information during the registration process. This information is stored in a central database (SQL) referred to as the "group practice management database" or GPMD. Access to this data by GIAC-HE staff is roles-based. Non-GIAC-HE staff is generally not given access unless a written release of information is obtained from the patient, or in legal instances, a court-issued request. Satellite (remote) offices have access via the GAIC-HE WAN, and physicians are requesting remote access via their home Internet connections. While HIPAA makes confidentiality of this information explicit (see discussion "E." below), there is a clear expectation by GIAC-HE's patients of confidentiality and protection of their data.
B. Baseline health data is collected from patients, referring physicians, and ancillary service providers. The primary storage of this data is non-electronic, i.e. the paper chart. Entry points for this info include oral, mail, fax, hand-delivery, telephone, and e-mail. Patient charts are stored in one of three (3) central file-rooms when not in use by the medical/nursing staff. Business office staff may also request access to the chart for insurance claim resolution. Chart location information ("chart tracking") is updated and stored in the GPMD.

   In anticipation of eventual migration to an electronic medical record (EMR), there are components of the MR stored electronically. Transcribed documents are stored (in Word and WordPerfect formats) on GIAC-HE's primary file and print server. Laboratory results are stored on the Lab Information Server (not currently on the LAN). Three practices are using EMR

software and SQL databases for their patients' visit documentation. Digital dictation voice files recorded by the radiologists are maintained for 14 days for preliminary report access (via dial-in to proprietary interface) prior to final printed report production. Access to all these "components" is limited to the users creating and maintaining the information, at least until it is placed in the paper chart. GIAC-HE's management has identified an "integration" system that will allow these (and future) components to be accessed as an EMR. Using a data-repository architecture, information from disparate sources for individual patients would be accessed from a web-browser-based interface. There has also been some discussion of extending access to the future EMR to GIAC-HE's partners and patients.

C. In addition to supporting the rendering of medical care, the patient's chart also serves as supporting documentation for claims for payment of services. GIAC-HE is an economic as well as health care operation. Approximately 80% of payments for services come from "third party" sources: insurance carriers, health plans, government-funded programs, Workman's Comp, and liability insurance. In all cases, GIAC-HE's invoice is an "insurance claim" submitted either electronically (+90%) or on paper. With few exceptions combining patient demographic information, services detail diagnosis, and the amount being billed produces these claims. This data is stored in the GPMD. Claim data is transmitted via modem to a claims clearinghouse for formatting and distribution to individual insurance carriers; paper claims are either shipped to the carrier by the clearinghouse, or back to GIAC-HE in the case of claims needing correction(s).

   As claims are processed (adjudicated) for payment, the insurance carrier may request additional or clarifying information. These requests are answered via phone, e-mail, fax, or mail.

D. Supporting GIAC-HE's clinical operations are:
   Executive Administration – responsible for management oversight of all non-physician employees, strategic and tactical planning, support of physician executive management, contract negotiation, corporate compliance and community relations. IT services utilized include e-mail (internal and external) with and without attachments, internal file and print services, and occasional access to medical records.
   Finance / Accounting – responsible for regular (monthly) reporting of all financial activities to Board of Directors, accounts payable and receivable, oversight of Business Office operations (patient accounting / claims), time and attendance tracking, payroll, banking, and contract review. IT services utilized include e-mail, internal file and print services, finance and payroll application server, modem and Internet access to business partner sites, and GPMD access and query.

Human Resources – responsible for non-physician staffing, benefits administration, employee relations programs, employment regulatory compliance, compensation and performance review administration, web-site content, employee training, and policies handbook maintenance. IT services utilized include email, hosted web-site access, file and print services, HR and payroll application server.
Physician recruitment / Credentialing – responsible for developing and maintaining provider credentials database, prospective identification of qualified candidates, planning and execution of interview visits, outside recruiter relations, and support to Board of Directors. IT services utilized include e-mail, file and print services, and access to variety of web-based resources.
Facilities and Supply – responsible for buildings and grounds maintenance and repair, mechanical systems, building security, shipping and receiving, mailroom, and central supply. IT services utilized include email, file and print services, Internet access.
Information Services – responsible for management of medical records storage, movement, and access control, network infrastructure planning and implementation, hardware (IT) acquisition and inventory, software licensing and distribution, application installation and support, network operations, and IT security.

E. As outlined in the "Transaction and Code Sets", "Privacy Rule, and proposed "Security Rule" sections of HIPAA regulations (see references listed for U.S. Dept of Health and Human Services), GIAC-HE's operations must be evaluated, documented, and as necessary augmented, to achieve regulatory compliance. As it moves toward HIPAA compliance, GAIC-HE has the opportunity to use information security best practices to streamline, protect, and add value to its information flow. HIPAA does not mandate that certain technologies are adopted or used – it does set clear expectations for using "appropriate" people, processes, and technology (Fried, Part 2, p. 1.5) to bring standardization, privacy, and security to healthcare information. GIAC-HE is not unique in the healthcare sector in embracing HIPAA rules as an opportunity to catch up in the areas of information security and data assurance. Fred Eisenberg, the senior director of security at Mt. Sinai NYU Health, and a former security officer in the financial industry, was quoted in the March 2002 issue of Health Data Management:

> "Financial companies have been in an electronic environment for a long time, so they have a lot of experience with electronic security and data quality assurance. The financial industry also has a security infrastructure that health care lacks. HIPAA is trying to bring that same focus on electronic security to health care." (Gillespie, p. 54)

Further, GIAC-HE's compliance encompasses the information that it transmits, receives, and shares with business partners. Therefore, attention to the "connections" with the business partners is essential for both information security and regulatory compliance.

GIAC-HE Critical Risk Identification

Risk 1 - Premature destruction or loss of patient medical record

Due to the transitional nature of GIAC-HE's medical record storage methods (from paper to electronic), this risk manifests itself in two forms. Also, because the medical record, regardless of storage method, represents the "crown jewels" of GIAC-'HE's operations, it is imperative that the integrity and accessibility of patient medical records be ensured for paper charts and for components that will eventually comprise an electronic medical record. Individual paper records must be protected from risk of loss resulting from theft, negligence, or intentional destruction. The medical record storage sites are at risk of loss due to fire or catastrophic building damage (wind, water). Finally, the data being stored for future EMR access is at risk due to hardware failure, backup/restore procedures, and unauthorized database/file access.

The patient medical record (paper or electronic) serves as the repository for information about the health care rendered by GIAC-HE. As such, it is possible that the existence of the record can be a true "life or death" issue. Short of this extreme, the ability of GIAC-HE doctors and staff to provide appropriate care is frequently tied to their ability to assess a patient's health care continuum. Patients and providers see the integrity of the medical record as essential for ongoing care, treatment, and quality of life. As the record of service and results, the medical record is also the supporting basis for all claims for payment. Failure to protect the paper medical record from premature loss or destruction would endanger patient lives, significantly reduce the quality of care, and threaten the financial health of the organization. Failure to protect the electronically stored components of a "future" medical record endangers GIAC-HE's successful transition to an EMR.

Threats, Vulnerabilities & Mitigation (Risk 1)

GIAC-HE's medical record policy establishes that there shall be one record for each patient and that all information pertaining to that patient's care and treatment be placed in that one record. As a result, patient charts are continually being moved in and out of the medical records department and between the various clinical offices of GIAC-HE (including remote sites). The vulnerability to loss of misplacement increases with the number of times a medical record is moved.

At any given time there may be tens of thousands of medical records "out of file" located on physician desks, nurse station counters, or in holding areas waiting for some action. While these areas are not generally "public", access does not currently require authentication or positive identification.

Mitigation of this risk could include:

- Central registration and "Visitor" badge issued to all persons on the premises for purposes other than receiving medical care (i.e., contractors, drug company reps, vendor reps, personal visitor, etc.).
- Basic information security and patient confidentiality agreement and acknowledgment for contractors.
- Lockable file storage area in each clinical office for medical records not being returned to medical records department.
- "Misplaced / Lost " medical record incident handling procedure.
- Minimize the number of building public entry points to reduce unmonitored, unauthorized traffic. All staff entry points should require some method of authentication (entry card, key-fob, or biometrics id).
- Restricted access to central filling areas (one per location).

GIAC-HE is geographically at risk for hurricane-related threats of wind (including tornado) and water (rain, flooding, and storm surge). The range of potential damage (loss) from this threat is broad – a few damp medical records from building leaks to catastrophic loss of a building and its contents. A Hurricane Preparedness and Action policy and procedures document must be reviewed and distributed annually no later than March 15 (Hurricane season runs from June through November). This is essential to ensure that losses are minimized in the event of a major storm striking the area. The business resumption plan should also be reviewed annually in preparation for "hurricane season". All responsible parties should be able to clearly articulate their specific actions when a storm event is forecast. These mitigating actions may include:

- Wrapping of filing shelves with plastic sheeting
- Moving records stored in flood-prone locations to higher floor or location
- Ensure all records "in-transit" between satellite offices are delivered or accounted for
- Designate a time and place for post-storm damage assessment and mitigation steps to reduce further exposure to loss

With respect to GIAC-HE's EMR components, the risk to computer systems, storage and archive media, and network infrastructure due to hurricane-related threats is parallel to that of paper records. In addition to the mitigation steps for paper records, the following steps should be taken:

- Distribution of two (2) complete sets of backups (all systems) to two different, geographically separated locations
- Routine testing and verification that the backup processes maintain data integrity and data can be successfully restored

- Controlled, clean shutdown of all network equipment, including PC's, printers, distribution equipment, and server room, followed by powering down and unplugging of all UPS devices.
- Given the increasing reliance on GIAC-HE network resources, a business resumption plan should be developed. While it may not be economically feasible to have redundant, backup systems available at all times, the who, when, how, and where of replacing network infrastructure and systems should be planned in advance. This process should include an annual review of applicable insurance policies versus expected replacement/resumption costs.

Risk 2 – Unauthorized access to and/or release of confidential data

For paper and electronic medical records, the risk that an unauthorized person gains access to "individually identifiable health information (HIPAA term – IIHI) exists due to inadequate authentication of the requesting party. GIAC-HE's patients expect confidentiality of patient health information. GIAC-HE expressly develops and implements policies and procedures to protect patient confidentiality. Loss of trust by a patient due to unauthorized release/access can result in the patient seeking health care elsewhere or legal actions against GIAC-HE. Additionally, as of April 13, 2003, GIAC-HE is required to have achieved compliance with HIPAA regulations set forth in "Standards for Privacy of IIHI" (the Privacy Rule). Significant fines, penalties, and sanctions are defined for failure to maintain the HIPAA privacy standards.

Threats, Vulnerabilities & Mitigation (Risk 2)

Paper records

In the current environment, the threat of unauthorized access to a medical record is magnified by the need for records to be in unsecured locations during their use for patient care. Throughout the workday, records can be found on physicians' desks, nurse stations, in the business office, and in transport containers. At any point that these locations are unattended by GIAC-HE authorized staff, the risk of unauthorized access rises substantially. As discussed in the Risk 1 assessment above, several of the mitigation steps for this vulnerability are building and visitor access controls. However, with the requirement to be able to provide access audit information (per HIPAA regulations) comes a need to:

- Establish clear roles of responsibility for the movement of medical records
- Assure accuracy and completeness in the GPMD Chart Tracking application.
- Define an incident procedure when a medical record is not in its expected location and document the results of any investigation.
- Periodic review of missing or misplaced record incidents to identify trends, patterns, and possible operational procedures.

Finally, the "records release" tracking system, used for logging and documenting release of information to parties outside GIAC-HE (physicians, insurance carriers, attorneys, etc.), must be used appropriately by well-trained staff.

Electronic Records

GIAC-HE's planned transition to an electronic medical record results changes the threat of unauthorized access or release of patient information. Because EMR access is related to a concurrent increase in the use of technology, there may be a tendency to rely solely on technological solutions to this risk. It is important that GIAC-HE not depend only on technology to mitigate these risks. Training, documented policies and procedures, and mechanisms for feedback and review must still play a central part of the security picture.

For GIAC-HE staff accessing EMR data, only a user name and password are required. This represents single-factor authentication and is insufficient to mitigate the risks associated with shared passwords, common-word (simple) passwords, or passwords discovered via social engineering. Contributing to the risk at GIAC-HE is the need for separate login accounts for multiple network services and applications – users are likely using the same or similar passwords for multiple logins (Novell, email, GPMD, etc.). There is also evidence that users are more likely to write down passwords when trying to remember multiple passwords. (Malik, p. 35)

To reduce this risk, GIAC-HE should:

- Develop a password policy that has owner and management support
- Make use of network and application password attributes to enforce the policy, including expiration frequency, character length, composition, number of invalid login attempts, password history, and inactivity timeouts.
- Evaluate and budget for a user-authentication system that raises the process to two-factor authentication – something the user knows and something the user either has or is.

While straightforward to develop, implementing any password policy that is perceived by users (especially physicians) as slowing down access will be a challenge. Training must include bringing GIAC-HE users to an effective level of understanding and ownership of their role in protecting their patients' information.

With respect to patient health information available via the public-facing web-server, it will be critical for GIAC-HE to establish defenses against unauthorized access. It is also important to take steps to isolate the web-server from the internal server network which will be the source of the master patient data repository so that attacks or illegitimate queries cannot be mounted from a compromised DMZ. Steps to mitigate this threat would include:

- Establishment of separate physical networks for the internal and DMZ servers in conjunction with database access controls based on allowed ports (firewall defined), thereby adding a layer of defense against unauthorized access.
- Following the "one server – one service" model for Internet-facing servers. This may involve expanding the number of actual servers required as GIAC-HE extends web-based access to its patients. This allows for true hardening of each server in the DMZ, as only the minimum services required are installed to support each application/database.
- Develop policies and procedures for monitoring database logs on a regular basis, watching for unusual login and query activity. A host-based IDS would be advisable for any DMZ-located server.
- Firewall policy monitoring to ensure that no "short-cuts" or other alterations are made without proper documentation and testing. Use of a tool that immediately alerts the ISO and Network Admin of any configuration change will help maintain the multi-layered defenses.
- Evaluation and selection of an encryption system to protect information being transmitted in response to patient queries, as well as a web-access server for maintaining a secure database of patients that have been authorized for use of GIAC-HE's Internet-facing services.

Risk 3 – Weakened virus and Internet defenses due to incomplete policy adherence

Due to the inconsistent application of standards and policies, PC workstations are at risk of being entry points for viruses, worms, and other Internet-borne attacks. Both PC configuration and acceptable use standards are at risk of abuse (and therefore weakening) when GIAC-HE "owner-users" (physicians) unilaterally bend the rules to accommodate their personal preferences and behaviors. Additionally, a risk exists that clinical support staff will emulate this user behavior. This results from the dual lines of authority and accountability for nursing staff. They "report" to their respective physician and to a member of GIAC-HE management.

Threats, Vulnerabilities & Mitigation (Risk 3)

Even in the absence of an EMR, GIAC-HE physicians rely on their PC's for e-mail, access to the Internet, hospital EMR, and continuing education tools. An interruption to this access can result in delays to the flow of information needed for an effective, efficient medical practice. As GIAC-HE transitions toward an EMR implementation, this risk will grow in its potential impact. Time and resources are consumed when a PC must be re-configured, software re-installed, or "treated" for virus infection. Overall effectiveness and respect for GIAC-HE's acceptable use policy is damaged when even one or two owner-users ignore or abuse the policy. In his article "4 Steps to Reducing Internet Abuse", Mike Foster

explains the importance of creating an environment that minimizes Internet abuse, which in turn can reduce Internet-related threats to GIAC-HE.

> "While technology solutions, such as monitoring filtering software, and sound Internet usage policies are great deterrents to Internet misuse, employees will ultimately conform to the established organizational culture. The culture breeds employees' attitudes, dictates how they behave at work, and instills in them a distinct work ethic.
> … Business owners and organizational leaders today have a responsibility to provide a positive culture in their organization, to lead by example, and to educate their employees about Internet misuse. …
> … In the end, company owners and managers must realize that Internet misuse is a cultural and human resources issue that cannot be solved by technology or policy alone. Instilling a positive organizational culture is the only way to guarantee that employees will be productive and that the company's goals will be met." (Foster, pp. 36-37)

There is a relationship between GIAC-HE's owner's support for acceptable use policies and the ability to use available tools to reduce the risk of infection, damage, or interruption of services. For example, if the policy outlines "safe" settings for Internet Explorer, but an owner changes those settings to accommodate use of web-sites of personal interest, then the layer of defense created by the policy has been breached. If the policy expressly prohibits use of GIAC-HE network resources by non-GIAC-HE persons, allowing family and friends to use the office PC (for any purpose) increases the risk of unauthorized data access and/or damage to data integrity. If a user takes steps to disable the anti-virus software on the desktop PC, a critical defense against Internet-borne viruses is eliminated.

Closer examination of the risk of virus infection at GIAC-HE reveals an external threat growing over time and a commensurate internal vulnerability that needs attention. The growing sophistication and frequency of virus-related threats, combined with the increased number of delivery methods, has coincided at GIAC-HE with a dramatic rise in the number of entry points (PC's) and easier, faster, cheaper, always-on Internet access. In 1995, GIAC-HE had no network, and only a handful of standalone PC's. In 2002, there are 280 desktop and notebook PC's (all of which have access to the Internet), and more than one hundred (100) users have an Internet mail address in the GIAC-HE domain. A key reason for having a relatively benign "viral history" is that GIAC-HE outsources the hosting of its Internet-mail services. But this has resulted in a false sense of safety and security. The eTrust IDS is capable of identifying virus and virus-like payloads in incoming email. It is unable to actually stop the email or an attachment from being delivered. GIAC-HE would be well advised to either update the IDS with email blocking features, or change email (Internet) hosting services to one that can provide such features. Without adopting a layered

defensive posture, GIAC-HE will continue to have single-point failure vulnerabilities.

PC-based virus protection is in place for users that use Internet e-mail. (GIAC-HE utilizes MS-Mail for PC Networks for "internal" email. Of course, this raises another set of issues related to ongoing accessibility, as Microsoft no longer supports the product.) A recent implementation of the Norton Antivirus Services Manager has strengthened this line of defense. Users are no longer involved in the virus-definition update process. However, Internet browsing activity is a weakness with the absence of control over configuration and security settings at the desktop level. To mitigate this risk, a standard desktop browser configuration can be developed, documented, and deployed (using Microsoft Internet Explorer Administrator's Kit - MS-IEAK).

In his January 21, 2002 Security Focus Online article "'Holistic' Enterprise Anti-Virus Protection", Paul Schmehl describes a well-rounded strategy "that can be used to help keep your enterprise relatively virus-free". Schmehl's recommendations are comprised of four (4) tactical areas: "Develop sound policies; protect the desktop [and servers]; educate the user; and protect critical services." (Schmehl, pp. 1 – 4)

For GIAC-HE, these tactics deserve significant focus and effort not just for defense against virus attacks, but also to reduce the vulnerabilities present as Internet use continues to grow. A strong defensive foundation in these two areas address weaknesses in the current environment – exposure to e-mail viruses, dangerous embedded content, "spyware", and other forms of malware. Just as important though is the ability to apply these tactics to increasingly complex external threats and vulnerabilities as GIAC-HE develops and extends access to patient information beyond its internal network via the Internet. Proper delineation of requirements for user authentication (strong password policies!), message non-repudiation, encryption of confidential and private information, roles-based access, server hardening and services "lock-down", and incident-handling procedures will be more effective if GIAC-HE has already mastered these four (4) tactics before the external threats and vulnerabilities are fully present. Building, implementing, and maintaining strong security policies based on these tactics will enhance GIAC-HE's transition to a safe and secure EMR.

Policy Evaluation: Internet Code of Conduct (Policy below extracted from Policies and Procedures Manual of author's employer)

GIAC Health Enterprises
INTERNET (VIA GIAC-HE LAN) CODE OF CONDUCT
July 1, 1999

I. Purpose

Access to the Internet (via GIAC-HE LAN) has been provided to staff members for the benefit of the organization and its customers. It allows employees to connect to information resources around the world; every staff member has a responsibility to maintain and enhance the company's public image and to use the Internet (via GIAC-HE LAN) in a productive manner. To ensure that all employees are responsible, productive Internet (via GIAC-HE LAN) users and are protecting the company's public image, the following guidelines have been established for using the GIAC-HE Internet domain (giac-he.com).

II. Policy

Acceptable Uses of the Internet

Employees accessing the Internet (via GIAC-HE LAN) are representing the company. All communications should be for professional reasons. Employees are responsible for seeing that the Internet (via GIAC-HE LAN) is used in an effective, ethical and lawful manner. Internet (via GIAC-HE LAN) Relay Chat channels may be used to conduct official company business, or to gain technical or analytical advice. Databases may be accessed for information as needed. E-mail may be used for business contacts.

Unacceptable Use of the Internet

The Internet (via GIAC-HE LAN) should not be used for inappropriate personal gain or advancement of individual views. Solicitation of non-company business, or any use of the Internet (via GIAC-HE LAN) for inappropriate personal gain is strictly prohibited. Use of the Internet (via GIAC-HE LAN) must not disrupt the operation of the company network or the networks of other users. It must not interfere with your productivity.

Communications

Each employee is responsible for the content of all text, audio or images that they place or send over the GIAC-HE Internet domain (white-wilson.com). Fraudulent, harassing or obscene messages are prohibited. All messages communicated on the Internet (via GIAC-HE LAN) should have your name attached. No messages will be transmitted under an assumed name. Users may not attempt to obscure the origin of any message.

Information published on the Internet (via GIAC-HE LAN) should not violate or infringe upon the rights of others. No abusive, profane or offensive language is transmitted through the system.

Software

To prevent computer viruses from being transmitted through the system there will be no unauthorized downloading of any software. All software downloads will be done through the IS Department. Requests for downloads should be sent via e-mail to the GIAC-HE Network Administrator or Director of Information Services.

Copyright Issues

Staff members on the Internet (via GIAC-HE LAN) may not transmit copyrighted materials belonging to entities other than this company. One copy of copyrighted material may be downloaded for your own personal use in research. Users are not permitted to copy, transfer, rename, add or delete information or programs belonging to other users unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action from the company or legal action by the copyright owner.

Security

All messages created, sent or retrieved over the Internet (via GIAC-HE LAN) are the property of the company, and should be considered non-confidential information. The company reserves the right to access and monitor all messages and files on the computer system as deemed necessary and appropriate. Internet (via GIAC-HE LAN) messages are public communication and are not private. All communications including text and images can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver.

Harassment

Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual or group's race, religion, national origin, physical attributes, or sexual preference will be transmitted.

Violations

Violations of any guidelines listed above may result in disciplinary action up to and including termination. If necessary the company will advise appropriate legal officials of any illegal violations.

Evaluation

Purpose of policy:

GIAC-HE's Internet Code of Conduct (ICC) was written and adopted in 1999 in recognition of the changing modes of communication being used by the organization. The primary goal of the policy is mitigation of risk of illegal, damaging, and non-productive activities related to Internet usage. By adopting a formal policy, GIAC-HE is giving the organization a vehicle for educating employees about their responsibilities and possible consequences for failure to follow the policy.

Background:

GIAC-HE established ISDN Internet access via its LAN in 1998. This was done in response to an increasing use (via modems) of Internet-based tools and resources by the medical staff and senior management. Internet e-mail was also becoming a "necessity" for communications with external business/clinical partners. After attempting to manage instances of "inappropriate" activities, it was clear to GIAC-HE management that a clear statement of acceptable Internet use must be adopted. The GIAC-HE's Board of Directors (physician leadership) approved the ICC policy upon recommendation of the Information Services Committee.

Evaluation:

On the whole, the ICC comes up short as an effective policy. What was included is clear, concise, and consistent with its stated purpose. In fact, the purpose is unambiguous, and the range of activities addressed by the ICC is fairly inclusive as far as user behavior is concerned. The policy is also consistent with other policies in its treatment of business communication (internal and external).

However, the policy items that are missing or not properly developed are significant, contributing to the risks associated with Risk #3 above. The in-completeness of the policy is a vulnerability in itself, as the ICC's expectations for user behavior and actions receive no support from procedures or technology – the only piece of the policy puzzle addressed is a list of do's and don't for people.

Specifically, the ICC policy is weak because:

- Some of the key terminology is broad or undefined. For example, "inappropriate" is used, but never explicitly described. "Unauthorized" implies there is a mechanism for obtaining authorization, but this is not addressed.
- The purpose does not address any pro-active steps and/or requirements for helping users conduct themselves properly. No mention is made of procedures or technology (browser configurations, email scanners, content filters, approved site list, etc.) that might assist users in adhering to the policy.

- No background information is provided in the policy. Inclusion would be helpful in establishing the context for the policy, as well as aiding in future revisions (as the context changes).
- There is no requirement for periodic review of the policy's applicability in relation to changing technology, access methods, and threats.
- The policy includes scant delineation of roles-based responsibility for the policy and its implementation.
- Retention of the data covered by the policy (email, browser logs, incident reports, protocol activity logs) is not addressed. How will these be stored, and on what media? Where will the archives be kept and for how long? Who has access to the data? Who authorizes retrieval of archived data?
- In the "Violations" section, who will advise "legal officials" and how and in what method? At a minimum there should be reference to associated policies that address "reportable" violations.
- No specific role is given the authorization to review activity logs or to determine that "inappropriate use is suspected".
- Viruses delivered via Internet e-mail, one of the greater risks to GIAC-HE, is not discussed in the ICC.

GIAC-HE Internet Code of Conduct – REVISED

I. Purpose

Access to the Internet has been provided to staff members for the benefit of the organization and its customers. It allows employees to connect to information resources around the world; every staff member has a responsibility to maintain and enhance the company's public image and to use the Internet in a productive manner. To ensure that all employees are responsible, productive Internet users and are protecting the confidentiality, integrity, and accessibility of GIAC-HE's information resources, this policy has been established for using the GIAC-HE Internet domain (giac-he.com).

II. Scope

This policy applies to any Internet communications using GIAC-HE network resources. All employees of GIAC-HE are subject to this policy as acknowledged by signed receipt of the GAIC-HE Policies and Procedures Manual, and by agreement to the responsibilities outlined in the Information Services and Patient Confidentiality Agreement.

III. Background

GIAC-HE network access to the Internet was established in 1998, in response to an increasing need for physicians and management staff to communicate efficiently with external partners and utilize resources available via the Internet. The Information Services Committee and the Board of Directors adopted the original Internet Code of Conduct in 1999 to address "inappropriate" Internet use and establish a basis for increased security from Internet-based threats. It is expected that this policy will evolve as the use of Internet resources changes and different risks and threats are identified.

IV. Definitions

Internet – in this document, refers to Internet access via any GIAC-HE network resources, regardless of location.
Inappropriate – outside the bounds of behavior normally accepted as ethical (business or medical ethics), lawful, and not damaging to others.

V. Policy Statements

1. Acceptable uses of the Internet: Employees accessing the Internet are representing the company. All communications should be for professional reasons. Employees are responsible for seeing that the Internet is used in an

effective, ethical and lawful manner. Internet Relay Chat channels may be used to conduct official company business, or to gain technical or analytical advice. Databases may be accessed for information as needed. E-mail may be used for business contacts.

2. Unacceptable uses of the Internet: The Internet should not be used for inappropriate personal gain or advancement of individual views. Solicitation of non-company business, or any use of the Internet for inappropriate personal gain is strictly prohibited. Use of the Internet must not disrupt the operation of the company network or the networks of other users. It must not interfere with your productivity. Inappropriate Internet use at GIAC-HE **may** include common web destinations offering sports reporting, weather information, auctions, job-listing/hunting, stock-trading, and other sites not related to GIAC-HE's mission or an employee's support of that mission as defined in their job description.
3. Communication: Each employee is responsible for the content of all text, audio or images that they place or send over the GIAC-HE Internet domain (giac-he.com). Fraudulent, harassing or obscene messages are prohibited. All messages communicated on the Internet should have your name attached. No messages will be transmitted under an assumed name. Users may not attempt to obscure the origin of any message. Information published on the Internet should not violate or infringe upon the rights of others. No abusive, profane or offensive language is transmitted through the system.
   a) E-mail messages sent and received via the Internet are the property of GIAC-HE. All incoming e-mail messages and any attachments will be scanned for virus or virus-like content prior to delivery to the GIAC-HE internal network. Messages found to be infected will not be delivered. The addressee and GIAC-HE's E-mail Admin will be notified via e-mail of undeliverable messages. The addressee will cooperate with the E-mail Admin.'s efforts to contact and advise the sender and document the virus incident. In the event an email message is intercepted be the addressee's desktop anti-virus software, the addressee will notify the E-mail Admin (or Network Admin) immediately by telephone and follow steps detailed in the GIAC-HE "Virus Incident Procedure".
   b) Internet e-mail accounts are established for physicians, physician extenders, managers, directors, and executive managers. All other requests for Internet e-mail accounts must be submitted by a manager to the Information Security Officer for authorization. (See GIAC-HE Internet E-Mail Request form)
   c) Only GIAC-HE approved e-mail client software will be used. Approved package, version, and configuration details are provided in the "GIAC-HE E-mail – Client Setup Procedure".
   d) Use of Internet Relay Chat (IRC) and streaming video and/or audio is allowed on a case-by-case basis, and must be work or continuing education-related. Requests for IRC access may be phoned or e-mailed to

the Information Security Officer for review, implementation, and documentation.

4. Software: To prevent computer viruses from being transmitted via the Internet there will be no unauthorized downloading of any software. All software downloads will be done through the Information Services department. Requests for downloads should be sent via e-mail to the Network Admin and copied to the Information Services Director. Each request will be documented in the Systems Support Log for review by the Information Security Officer. Requests must include a statement of justification and manager approval (for non-physician requests). Proper purchase request authorization must accompany requests requiring shareware or proprietary license fees.
5. Copyright Issues: Staff members may not transmit Internet copyrighted materials belonging to entities other than GIAC-HE. One copy of copyrighted material may be downloaded for personal use in work-related research. Users are not permitted to copy, transfer, rename, add or delete information or programs belonging to other users unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action by GIAC-HE or legal action by the copyright/license owner.
6. Security:
   a) All messages created, sent or retrieved over the Internet are the property of GIAC-HE and should be considered non-confidential information. [With respect to non-confidentiality, exceptions to this statement may be listed upon implementation of VPN (authentication and encryption) capabilities between GIAC-HE sites and/or business partners. GIAC-HE reserves the right to access and monitor all messages, files, and Internet sites accessed as deemed necessary and appropriate for Internet Code of Conduct Policy enforcement. All Internet communications including text and images can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver.
   b) All devices used to communicate via the Internet will be configured according to the most recent version of the GIAC-HE "Web-Browser Configuration" Procedure. Generally, GIAC-HE will follow the recommendations of C.E.R.T. (Computer Emergency Response Team: www.cert.org) and the Internet Storm Center (www.incidents.org), as well as other sources as identified by the GIAC-HE Information Security Officer, in establishing browser and Internet e-mail configuration requirements. Further, no Internet access is allowed except via a firewall-protected, NIDS-monitored connection to a GIAC-HE designated Internet Service Provider. As threats and vulnerabilities change, the configuration may be altered to maintain acceptable risk levels.
   c) A network-based Intrusion Detection System (NIDS) will monitor Internet communications, log browsing activity, scan e-mail attachments for

viruses, and generate routine and ad-hoc reports (based on GIAC-HE management requirements). Specific NIDS configuration and management will be the responsibility of the Information Security Officer, and documented in the "GIAC-HE NIDS Operations and Procedures". Information Services employees with access to the NIDS logs and reports will only do so with explicit authorization from the ISO or GIAC-HE's Executive Director or Medical Director. NIDS logs will be archived on a routine basis according to procedures included in the "NIDS Operations and Procedures" document.

d) GIAC-HE uses a subscription-based "prohibited sites" approach to blocking access to certain objectionable or inappropriate web-sites. Internet users may request access to a "prohibited" site through their manager or, in the case of physicians, directly to the ISO. All such requests will be in writing, and documented in the NIDS Incident and Change Log.

7. Harassment: Harassment of any kind is prohibited. No messages with derogatory or inflammatory remarks about an individual or group's race, religion, national origin, physical attributes, or sexual preference will be transmitted.

8. Disclaimer of Liability: (Orley, page 39)

> GIAC-HE is not responsible for material viewed or downloaded by users from the Internet. The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. In addition, having an Internet e-mail address may lead to receipt of unsolicited e-mail containing offensive content. Users using the Internet do so at their own risk.

9. Violations: Violations of any guidelines listed above may result in disciplinary action up to and including termination, according to GIAC-HE Disciplinary Actions Policy. If necessary GIAC-HE will advise appropriate legal officials of any illegal violations. Such notification will be in writing, over the signatures of the Executive Director and President of GIAC-HE, and with prior review by GIAC-HE legal counsel.

VI. Policy Implementation and Review

1. New employees: Prior to use of GIAC-HE network resources, this policy will be reviewed with each new employee of GIAC-HE.

2. Periodic security training will be given annually to all employees of GIAC-HE, including a review of this policy.

3. Updates and review of this policy are the ongoing responsibility of GIAC-HE's Information Security Officer, and will be performed at least every six months or more frequently as needed to respond to technology and operational changes. Associated procedures will also be amended as needed to afford the intended security protections.

(End of revised ICC policy)

PC – Internet Web Browser Security Configuration Procedure

Purpose:

This procedure provides instructions for configuration of Microsoft Internet Explorer (MSIE) 6.0 on GIAC-HE PC's.

Scope:

Any PC with access to the Internet via GIAC-HE network resources will have its browser (MSIE-6.0) software configured according to this procedure. This configuration is based on information security practices designed to: 1) mitigate current Internet-based threats and 2) enable GIAC-HE users to be productive Internet participants within the guidelines of GIAC-HE's Internet Code of Conduct policy.

Revisions and Updates:

It is the responsibility of GIAC-HE's Information Security Officer to revise and update the configuration procedure as Internet-based threats evolve and as browser software changes. At a minimum, a review of this procedure will be performed every six- (6) months, using currently available vendor-independent recommendations as well as Microsoft supplied updates and security alerts. More timely update(s) are expected when notice of a new vulnerability is received and the risk to client PC's is rated as medium or high.

Configuration changes will be tested and documented fully prior to rollout to production PC's. Further, the ISO, or Network Admin in the ISO's absence, will monitor weekly security alert newsletters from C.E.R.T. and SANS.

Security Goals:

- Mitigate the threat of harmful content being accessed or introduced into GIAC-HE's network via Internet browsing.

- Reduce the likelihood that information related to patient health care or GIAC-HE's business operations is collected by unauthorized individuals.
- Disallowing untrusted scripts, web-based programs and updates to minimize the web-based trojan horse threat.

- Defining Internet zones to facilitate safe, appropriate browsing for GIAC-HE users.
- Timely delivery of browser updates, patches, and configuration settings to user PC's.
- Ensure awareness of newly discovered vulnerabilities and take action to mitigate.

Internet Explorer Zone Settings – Overview

1. Internet (default): Sites not explicitly included in the Trusted Sites zone. Does not include Restricted zone sites, which are blocked using URL filtering at the NIDS.
2. Trusted: Sites that have been verified by the ISO as being "safe" for GIAC-HE business purposes. Less restrictions are placed on these sites to enhance usability and functionality. A master list of Trusted site domains will be maintained by the ISO (or designee) and updated as needed based on user requests.
3. Restricted: Sites categorized by URL subscription service as having no value to GIAC-HE's business objectives, or known to practice poor security precautions.

Steps:
[Note: The steps below describe actions for establishing security settings on an individual PC. It is anticipated that GIAC-HE I.S. staff will utilize Microsoft Internet Explorer Administrator's Kit 6.0 for deployment to networked PCs. IEAK 6.0 info: http://www.microsoft.com/windows/ieak/techinfo/deploy/60/en/]

1. On the Windows desktop, single right-click on the Internet Explorer icon. In the resulting context menu, choose "Properties". This will open "Internet Properties" window.
2. Single left-click the "Security" tab to access Zone Settings. Highlight the security zone being updated (Internet, Trusted, or Restricted), and then single left-click on the "Custom level" button.
3. Using the Zone Properties Matrix below, customize the settings.
4. After the Security zone customizations have been completed, single left-click on the "Advanced" tab to access Advanced Properties window.
5. Use the Zone Properties Matrix to update the settings as documented. (Advanced settings not documented in the Security Zone matrix are addressed in other procedures.)
6. When all settings have been updated, single left-click on the "OK" button at bottom of Internet Properties window to save the changes.

Zone Properties Matrix

	Zone Settings		
Property	**Internet**	**Trusted**	**Restricted**
Download signed ActiveX controls	Prompt	Enable	Disable
Download unsigned ActiveX controls	Disable	Prompt	Disable
Initialize & script ActiveX controls not marked as safe	Disable	Prompt	Disable
Run ActiveX controls and plug-ins	Admin approved	Enable	Disable
Script ActiveX controls marked safe for scripting	Prompt	Enable	Prompt
File downloads	Disable	Disable	Disable
Font downloads	Enable	Enable	Prompt
Java permissions	High	Medium	Disable
Access data sources across domains	Disable	Prompt	Disable
Allow META REFRESH	Disable	Enable	Disable
Display mixed content	Prompt	Prompt	Prompt
Don't prompt for client cert selection …..	Disable	Enable	Disable
Drag/drop or Copy/paste files	Disable	Enable	Disable
Installation of desktop items	Disable	Disable	Disable
Launching programs & files in an IFRAME	Disable	Prompt	Disable
Navigate sub-frames across different domains	Prompt	Enable	Disable
Software channel permissions	High	Medium	High
Userdata persistence	Disable	Disable	Disable
Active Scripting	Disable	Disable	Disable
Allow paste operations via script	Disable	Prompt	Disable
User authentication	Prompt	Prompt	Prompt

Advanced Properties Matrix

Property	Setting
Enable install on demand (IE)	Uncheck
Enable install on demand (other)	Uncheck
Enable third-party browser extensions	Uncheck
Play sounds in web pages	Uncheck
Play videos in web pages	Uncheck
Check for server certificate revocations	Check
Check for signatures on downloaded programs	Check
Warn if changing between secure and not secure mode	Check

(Cooper, 20 Feb 2002 "Webinar" presented by TruSecure)

In applying the above security options, the GIAC-HE ISO may determine that particular Internet users may require less restrictive settings in order to realize needed functionality at certain sites. Such cases will be documented and a corresponding properties matrix added to this procedure.

(End of Configuration Procedure)

References

Baczewski, Philip et al. E-Mail Virus Protection Handbook. Rockland: Syngress Publishing, Inc., 2000.

Convery, Sean and Saville, Roland. "Extending the Security Blueprint to Small, Midsize, and Remote-User Networks." Cisco Systems, Inc. 25 June 2001. URL: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safes_wp.htm (6 April 2002)

Cooper, Russ. "Coffee with Cooper Webinar Series on Microsoft Security." Presented by TruSecure, 20 Feb 2002. (online Internet seminar attended by author) http://www.trusecure.com/html/news/press/2002/prcooperwebinar021802.shtml

Fried, Stephen. "SANS Security Leadership, Parts 1 & 2." SANS Institute 2002, SANS-ISO Conference/Training Materials: San Diego, 25 Feb 2002.

Foster, Mike. "4 Steps to Reducing Internet Abuse." Contingency Planning and Management April 2002 (2002): 36 – 37.

Gillespie, Greg. "Defining the Roles of HIPAA Officers." Health Data Management" March 2002 (2002): 52 – 56.

Hare, Chris and Siyan, Karanjit. Internet Firewalls and Network Security, Second Edition. Indianapolis: New Riders Publishing, 1996. Pages 97 –157 (Designing a Network Policy)

Kerby, Fred. "Defense in Depth." SANS Institute 2002, SANS-ISO Conference/Training Materials: San Diego, 25 Feb 2002.

Malik, W. "Does your password policy reduce enterprise security." Network Administrator's Security Resource Guide. Louisville: TechRepublic, 1999-2000. Pages 34 – 35.

"Microsoft Internet Explorer Administrator's Kit Help." Microsoft Corp., 1999-2001 http://www.microsoft.com/windows/ieak/techinfo/deploy/60/en/ (21 Feb 2002)

National Security Agency (Systems and Network Attack Center). The 60 Minute Network Security Guide. Ft Meade: NSA (USA), 2001.

Nutter, Ronald. "Deploying Internet Explorer 5 Using the Internet Explorer Administration Kit." Microsoft TechNet 2002 [No date given for article]. Accessed 08 April 2002. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/ie/deploy/depieak.asp

Overly, Michael R. E-Policy: How to Develop Computer, E-mail, and Internet Guidelines to Protect Your Company and Its Assets. New York: SciTech Publishing, Inc., 1999.

Schmehl, Paul. "'Holistic' Enterprise Anti-Virus Protection." Security Focus Online, 21 January 2002. URL: http://online.securityfocus.com/infocus/1538 (26 March 2002)

U.S. Department of Health and Human Resources. Standards for Privacy of Individually Identifiable Health Information; Final Rule. Washington DC: National Archives and Records Administration, 2000. Federal Register 45CFR Parts 160 and 164.

U.S. Department of Health and Human Resources. Health Insurance Reform: Standards for Electronic Transactions; Final Rule. Washington DC: National Archives and Records Administration, 2000. Federal Register 45CFR Parts 160 and 162.