Global Information Assurance Certification Paper

Information Security Officer Training

GISO – Practical Assignment

Version 1.2 February 9, 2002

GIAC Healthcare

Submitted by

Jay Rankin

Table of Contents

Abstract

GIAC is a physician office practice, specializing in family medicine. The practice provides a broad spectrum of office-based medical care for people of all ages. In the competitive business of healthcare it is necessary to secure market share. Increasingly a prime mechanism for providers in private practice to achieve this is to have timely and easily accessible patient information for their clinical use and the rapid submission of claims for reimbursement via a computer network.

The intention of this paper is to inform the reader about the business of the GIAC Healthcare, the supporting IT infrastructure and overall security posture, including the critical IT security risks to the practice and the steps GIAC has taken to mitigate these risks. These points will be discussed within the framework of GIAC's operations.

Access to the systems of GIAC is protected by a username/password combination. Inappropriate access to patient or organizational information risks the loss of patient trust, causing potential harm to patients and places GIAC vulnerable to potential civil and regulatory action. Management of this combination is critical to the security of these systems. A policy and procedure for the management of user sign-ons is proposed in this document.

Assignment 1 – Describe GIAC Enterprises

GIAC Overview

GIAC is a physician office practice, specializing in family medicine. The practice provides a broad spectrum of office-based medical care for people of all ages from an office suite nearby the local medical facility. The same doctor usually cares for an entire family and provides most of their care. If complicated problems arise, this provider connects the patient with a specialist or arranges for admission to a medical facility. The services that are provided by GIAC include:

> Pregnancy Care & Delivery
> Pediatric Care: childhood illness and routine child care
> Adolescent Care: health maintenance, injuries, sports medicine
> Women's Care: cancer screening, birth control, menopausal concerns, pre-pregnancy planning
> Adult Medical Care: high blood pressure treatment, heart disease prevention & treatment, cancer screening, diabetes care
> Surgical Care: vasectomy, sigmoidoscopy and other minor surgeries Checkups and Health Screenings
> Specialty Clinics: prenatal screening, endocrinology, dermatology, and osteopathic manipulation (held on a weekly or monthly basis)
> Geriatric Care: chronic disease care, functional assessments, home visits, nursing home care. [Author]

In the competitive business of healthcare it is necessary to secure market share. Increasingly a prime mechanism for providers in private practice to achieve this is to have timely and easily accessible patient information for their clinical use and the rapid submission of claims for reimbursement. Ensuring that patient information is current and accurate has become critical to both their clinical and fiscal operations. To this end GIAC has recently invested in a network and electronic medical record for their office. In defining the scope of this project the practice's decisions were greatly influenced by the pending implementation of new regulatory requirements.

Because computerized systems permit the movement of large amounts of patient information concerns have been raised regarding the appropriateness of its use by the various stakeholders involved. Because the stakeholders represent different needs, no consensus exists regarding the legitimacy of the information that is processed and how it is used. [NRC, 80] Into this arena has now come the Health Insurance Portability and Accountability Act of 1996, known as HIPAA. The act speaks to two areas that directly affect GIAC and its operations.

First, the act establishes common standards for the submission of reimbursement claims. All providers are now required to adhere to the ANSI (American National Standards Institute) ASC (Accredited Standards Committee) X12 standards for all submissions.

Second, the legislation provides regulatory standards for the confidentiality, availability and integrity of patient information and requires healthcare providers to meet these standards. The act further establishes sanctions for the inappropriate release and/or use of individually identifiable patient information. The actual implementation requirements and technology are not specified, leaving each organization to determine how best to meet the requirements and intent of the act. [Gue] The act provides for three concepts to ensure the standards are effective and applicable.

Solutions to HIPAA compliance are to be technology neutral. This allows organizations the flexibility to determine their solutions and focus on achieving the desired end results of security and compliance. Solutions must be scalable. Scalability allows each organization to meet compliance standards that are appropriate to their situation and size. The solutions for an organization must be comprehensive. This has been defined as managing four layers or categories to meet compliance. These layers are defined as:

> Administrative procedures.
> Physical safeguards
> Technical security services
> Technical security mechanisms

As required by this legislation, GIAC, has developed its own HIPAA compliance plan. Because a risk assessment of all systems in use by a healthcare entity is required by HIPAA the selection of information technology to support the practice's operations has been directly influenced by this legislation.

Business Operations:

The medical practice at GIAC includes a staff of physicians, physician extenders and support staff, numbering 40 users. Patients are assigned to a physician who is part of a care team, that includes the primary physician, a physician extender, and clinical and administrative support staff. Although patients are assigned a primary provider, the physicians and extenders provide on-call coverage for each other's patients.

A typical flow for an office visit would include the following interactions:

1. The office visit is scheduled with administrative support staff in the practice's clinical information system.
2. The patient is checked in upon arrival at the office. The check-in includes verification of demographic and insurance information which is entered into the clinical system and interfaced to the administrative information system.
3. The patient is seen by clinical support staff and a provider in an examination room.
4. The patient's records are updated with the results of the visit with notations regarding any follow-up testing made into the clinical system.

5. The visit is prepared for billing in the administrative system through the use of the input of Current Procedural Terminology (CPT) coding for the services that have been rendered. These codes are used by the payers of benefits to determine the appropriate level of payment to the organization for services. Claims and requested justification for services are then sent to various state and private payers for reimbursement via a third party insurance clearinghouse through file transfer protocol (FTP).
6. Follow-up laboratory testing and transcribed results are interfaced into the practice's clinical system from contracted reference entities.
7. Scheduling of any needed follow-up visits, relevant health information and any needed reminder notices are generated the clinical system.
8. Patients call in for follow-up consultations when testing has been completed or a health problem arises.
9. Questions regarding care, notifications of appointments and much of the office correspondence is accomplished through the Exchange Email system.

Throughout the process the access to patient information is critical. The provision of care, the meeting of regulatory requirements, claims submission, reimbursement justification, accrediting processes and governmental reporting mandates all require that the provider and support staff have secure and ready access to organizational and patient information. Disruption of the information flow or compromise of confidentiality would constitute a serious risk to both the clinical and administrative operations of GIAC.

As this generalized flow of information shows that a potentially large number of organizations collect, process and store health information. These organizations are not limited to healthcare providers, but also include insurance companies, employers, utilization review groups, state organizations and public health reporting groups. [NRC, 74]

The current systems are the result of a steady movement over that past few years that sought to gain efficiencies from the computerization of various processes in the practice. GIAC has followed the traditional path of many healthcare organizations, bringing in first a financial system, then a system to support the clinical operations. These two systems are now well established in the practice and additional mechanisms to leverage technology are being sought.

To provide necessary information GIAC has implemented a network throughout their offices. Critical to the practice's operation are two systems, one clinical and one administrative support. These two systems provide GIAC with its core computing systems that house the "crown jewel" of the organization, clinical and financial patient information.

GE Medical Systems' Logician product provides the practice with an electronic medical record system that enables physicians and support staff to schedule and document patient encounters, streamline clinic workflow, and securely exchange clinical data with

other providers and information systems within the practice. [Log] Laboratory results and transcribed reports are interfaced by HL7 standard for inclusion in the patient record from contracted testing services. The information is ported to the Logician system automatically by a FTP client with a scheduler over POTS. Access to the Logician application is made via a citrix session. Logician system has provided the necessary privacy and security features allowing GIAC to meet HIPAA privacy, administrative and technical requirements.

The second system is the Millbrook Practice Manager system. This system is interfaced via an HL7 interface to the Logician system that is used to schedule patient visits, capture necessary patient demographic and financial information and record clinical information. The Millbrook system compliments the clinical system, providing for the various administrative management functions needed for the practice to be viable. These include maintenance of current patient demographic and financial information, claims filing and reporting, accounts receivable and payment posting. In addition to privacy and security standards the Millbrook system has completed development of claims and remittance formats using the current ANSI (American National Standards Institute) ASC (Accredited Standards Committee) X12 standards. Eligibility and eligibility response files are mapped to the ANSI ASC X12 format as well, providing compliance with HIPAA. [Mill] The movement of files for claims and reimbursement between the Millbrook system and third party payers is performed by a FTP client with a scheduler over POTS . The Millbrook system has provided the necessary privacy and security features allowing GIAC to meet HIPAA privacy, administrative and technical requirements.

As part of its move to streamline patient visits and to better utilize provider time, GIAC has recently deployed a wireless network within its offices. The practice has begun using this network with handheld devices for use by the providers in the patient examination rooms. The benefits they anticipate from this deployment include greatly increased user mobility and flexibility, allowing the real time retrieval of information, documentation of care and the posting of new orders for patients in as part of the patient examination process. Compared to wired networks this system may be installed much more rapidly and in a more scalable manner. As work areas change the wireless network is extremely flexible in its ability to adapt and be reconfigured based on the needs of GIAC. [NISTW, 3-12]

External access to the GIAC network is provided to the providers through a VPN using IPsec protocol with password authentication. The availability of patient information to on-call providers is critical to rendering patient care. The GIAC providers regularly access patient information remotely during “off hours” when answering calls from patients of their own and other providers in the practice via a citrix client on their home PC’s.

IT Infrastructure

GIAC’s network is managed by a locally contracted IT firm. GIAC has executed a Business Partner Agreement with the firm as required by HIPAA legislation. The

agreement defines the role of the firm in system management and the steps the firm is to take protecting GIAC's organizational and patient information. The services include network management, backup archiving and webmaster management for the practice's Internet homepage.

Because access to patient information is critical in treatment, the IT support company provides 24x7 coverage for the network support. The support IT users use PC Anywhere once they have authenticated themselves over the VPN connection, to provide remote support. The on-call providers have a citrix client installed on their home PC that allows them to access the clinical applications once they have authenticated themselves over the VPN connection.

The GIAC network has evolved over a number of years. It's current configuration is designed to provide as much flexibility for the practice as possible within the fiscal constraints they have to work with. All external traffic is routed through the Cisco 2611 router. This router performs basic filtering then sending traffic to the SOHO3 firewall which maintains the VPN access portal and routes DMZ traffic to the appropriate port. The DMZ contains a single service server:

A. GIAC's webserver, an Apache server running Red Hat 7.3 hosts the practice's homepage. This service provides an external point of contact for the local populace to become aware of the services that GIAC provides. To add value to these pages GIAC provides regular updates of general medical information to their webmaster at the IT support company for updating of the pages.

The server has been hardened to only allow the minimum services necessary for its individual tasks.

Remote users VPN in over a SSL session to the SOHO3 firewall via a SSL session (take out) with the VPN service using triple DES 168 bit encryption. The username/password combination is required for access to the network, with authentication taking place on the Primary Domain Controller. Network policy has been defined to provide a reasonable level of security while not compromising access for users.

A. Network policy requires a mixture of upper/lower case alpha characters mixed with numbers with a minimum length of 8 characters.
B. Passwords expire in 90 days.
C. Passwords are retained in history for 4 cycles.
D. After four login failures the account is locked out.
E. Lockouts are set expire after 30 minutes. This is to allow user access during off hours, when taking call.

Access to the application servers is made based on the privilege set defined in a user's Windows 2000 profile. Access to the applications themselves is based on the profiles defined in each application. The SOHO3 firewall is ISCA certified and performs stateful

packet inspection of all internet traffic and a Network Address Translation (NAT). External network address of 144.xx.xxxx.xxx is NAT'd to the server sub-nets 172.xx.xxx.xx and the end user sub-nets 192.xx.xxx.xx. Traffic between the two subnets is routed by the internal Cisco 2611 router.

Internal traffic on the 172.xx.xxx.xxx sub-net is routed by the Net Gear GS516T switch. Traffic to the wired network end user devices is controlled by the Net Gear FS524S stackable switch. The wireless network is made possible by a Linksys WAP11 access point that is located outside the firewall. Users of wireless devices VPN in to access to applications. The wireless devices are configured with a citrix client and require authentication to access the network.

The mail server, PDC and application servers are all on separate sub-nets (above). Each Windows 2000 server is configured to run the minimum necessary services for the supported application.

Application Servers

Port	State	Service
25/tcp	open	smtp
80/tcp	open	http
135/tcp	open	loc-srv
139/tcp	open	netbios-ssn
443/tcp	open	https
445/tcp	open	microsoft-ds
1031/tcp	open	iad2
1521/tcp	open	oracle
2301/tcp	open	compaqdiag
3389/tcp	open	msrdp
5631/tcp	open	pcanywheredata

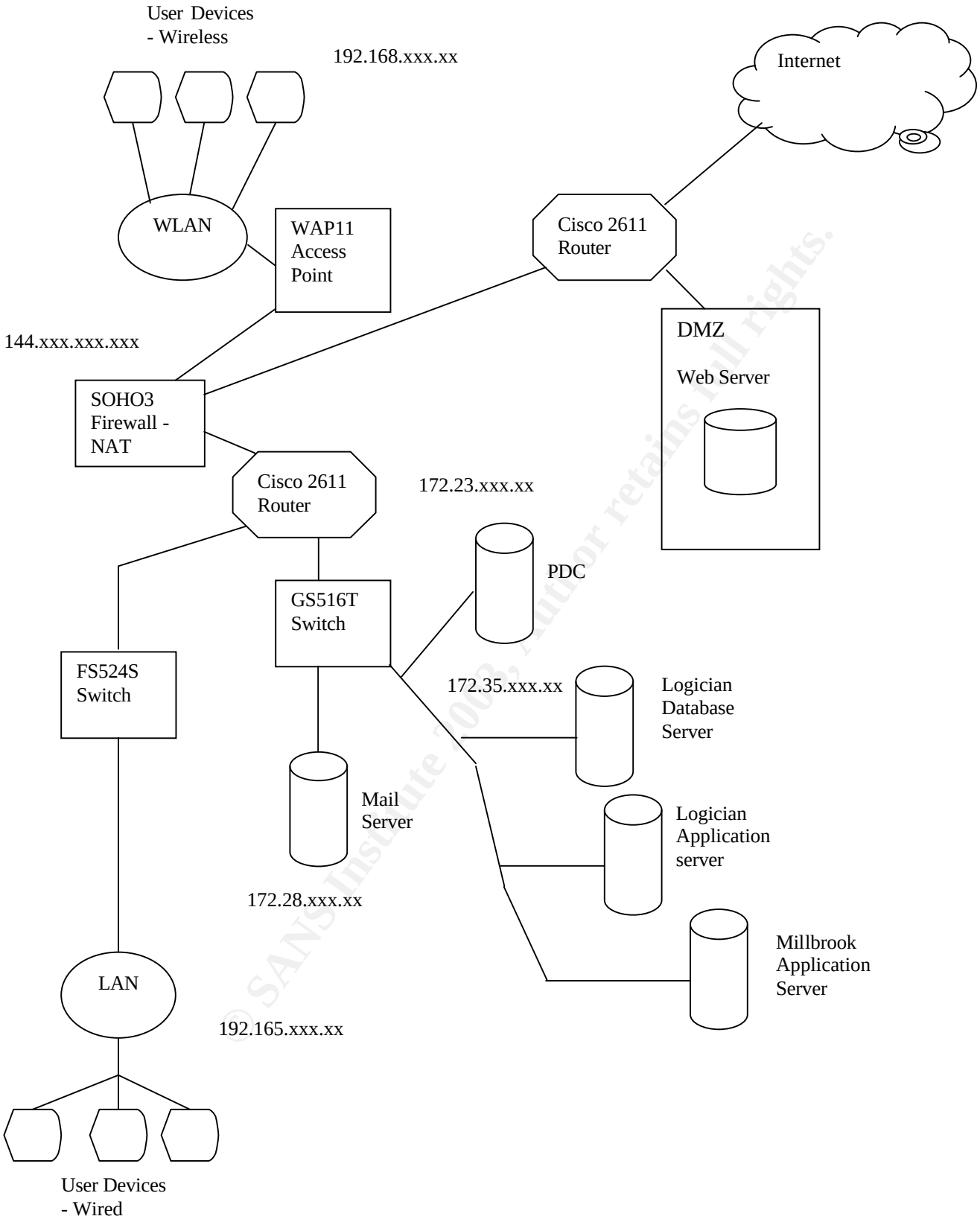
Mail Server

Port	State	Service
25/TCP	Open	smtp
27/TCP	Open	etrn
110/TCP	Open	POP3
119/TCP	Open	NNTP
135/TCP	Open	loc-srv/epmap
139/TCP	Open	netbios-ssn
143/TCP	Open	IMAP
389/TCP	Open	LDAP
563/TCP	Open	NNTP over SSL
593/TCP	Open	http-rpc-epmap
636/TCP	Open	sldap
993/TCP	Open	s-imap
995/TCP	Open	pop3s
1059/TCP	Open	nimreg
5631/TCP	Open	pcanywheredata

These systems are supported by an Microsoft Windows 2000 network running active directory. All connections to the network require authentication. Functional area managers (FAM) have defined the tasks necessary for the performance of the various activities in the practice and tailored privileges to these profiles for access to both the servers and applications.

Anti-virus protection is layered. The firewall performs the initial scans and blocks potential incoming virus laden traffic by stripping potential executables, zip and scripting files before any email is allowed into the network. The Exchange mail server is provided with McAfee GroupShield software for anti-virus scanning. End user devices are protected with automatically updating McAfee VirusScan.

Given the size of GIAC the implementation and on-going support of an intrusion detection system is not considered fiscally feasible at this time. Future plans may include this functionality. At this time auditing services have been enabled for the network. The IT support company provides a regular review of these logs for any suspicious activity. In addition the company provides for regular checks of critical files, to detect inappropriate activity or updates via a MD5 hash routine.



Network

Product	Model/Version/Vendor	Operating System	Location	Application
Sonic Firewall	SOHO3	5.1.7.0	Network Perimeter	VPN Firewall
Cisco Router	2611	IOS 11.3 (T)	Network Perimeter	Router
Cisco Router	2611	IOS 11.3 (T)	Internal	Router
Netgear	FS524S – 24 port 10/100 Mbps switch		Internal	Multi Service Stackable Switch
Netgear	GS516T – 16 port 100/1000 Mpbs gigabit switch		Internal	Multi Service Switch
Linksys	WAP11	1.06	External Network	Wireless Access Point

Servers And Hosts

Product	Model/Version/Vendor	Operating System	Location	Application
Logician	Dell 600SC	Windows 2000 Server SP2.	Internal	Database Server – Oracle 8i
Logician	Dell 600SC	Windows 2000 Server w/ Terminal Services w/ SP2) **and** (Citrix MetaFrame v1.8 SP2 Feature Release 1)	Internal	Application Server
Millbrook Practice Manager	Dell 600SC	Windows 2000 server SP2	Internal	Application server
Microsoft Exchange Server	Microsoft	Windows 2000 server SP2	Internal	Mail Server
Microsoft Server	Microsoft	Windows 2000 server SP2	Internal	Primary Domain Controller
Web Server	Apache	Red Hat 7.3	DMZ	Web Server IE 5.5
Workstations	Dell Dimension 4550	Windows 2000	Internal	User workstation
Wireless Workstations	Compaq CE Tablets	Windows 2000	Internal	User wireless workstation

Assignment Two: Risk Identification

Introduction:

"Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization." [NIST, 8] The primary area of risk for GHA revolves around patient information, its generation, storage, use and access. An examination of the threats and vulnerabilities for the protection of patient information is useful.

"Threats to the information processes may be categorized as natural, human or environmental." [NIST, 12] While natural and environmental issues must be addressed, for the purposes of this discussion the focus will be on the human threat. Possible human actions span the range of inadvertent mistakes to malicious actions specifically designed to cause harm.

"Vulnerabilities are those flaws or weaknesses in the system that could be exercised either accidentally or maliciously to cause a security breach." [NIST, 15] For the threat to materialize into risk a vulnerability needs to exist.

"Healthcare systems by their nature of desiring to be accessible, have historically been prone to vulnerabilities. This has caused privacy to not often be a market differentiator." (NRC, 5) In reviewing the threats mentioned, the lack of strong authentication, failure to sign-off sessions, the lack of audit logs and disgruntled employees are always necessary to be aware of. In addition, an organizational culture that does not continually emphasize the need to keep patient information confidential or has the "it can't happen here" attitude all contribute to the increase of risk to systems. The annual 2002 CSI/FBI survey has shown computer related crime and attacks on systems continues, with the financial toll increasing. "While healthcare organizations compose only a small percentage of the respondents to various surveys, the reports do indicate the increasing vulnerability of systems attached to public infrastructure such as the internet." [NRC, 55]

The crown jewel of the GIAC physician practice is that of patient information. To provide appropriate safeguards for this information GIAC has sought to build a network centered around the Logician and Millbrook applications that provides for a reasonable level of security.

Three areas of risk have been identified in connection with the critical nature of the of patient information needed by the practice.

1. The unauthorized release of patient information from the wireless network.
2. The unavailability of patient information due to virus/malicious software.
3. The unavailability of Information Due to Poor Backup and Recovery Process.

Risk One: Unauthorized release of patient information from the wireless network

The first risk is that of unauthorized release of patient information. The authorized release of patient information is based on the patient providing an informed, voluntary and competent written consent to the organization.

The are four areas of concern for GIAC:

1. "The release of patient information, first and foremost, if released to the wrong party may cause harm to the patient. Information dealing with mental health, substance abuse or sexually transmitted diseases may result in the loss of employment, insurance or social status." [Clark, Bresee, 71]

2. For the organization, the unauthorized release of information jeopardizes its' reputation and so risks the loss of trust in the community and subsequent loss of its core business, healthcare. Patients will not seek care where they do not feel their confidential information will be protected. [Clark, Bresee, 71]

3. The risk of regulatory action, primarily in the form of the Health Insurance Portability and Accountability Act of 1996, known as HIPAA, is now established.

4. The final concern, that of civil actions in the courts, has a number of precedents, with the rights of patients and the confidentiality of their information being paramount. [Clark, Bresee, 71]

All four concerns have the potential to severely damage GIAC's ability to function as a healthcare practice.

The potential risk of unauthorized release or access to patient information has been significantly increased with the introduction of the wireless technology to the GIAC network. The deployment of the wireless network to complement the increased functionality of the clinical systems adds a new dimension to protecting patient information and the network from unauthorized access. Unlike wiring which within the facility is acceptably secure, wireless networks are not limited to the four walls they reside in. "An attacker only has to be in the proximity of the wireless network, often without entering the building of the potential victim." [Zeltser, 43]

The vulnerabilities which are inherent in the current version of most wireless installations include:

A. Vendor supplied security features are not enabled.
B. The encryption standards currently part of the IEEE 802.11b standard have been found to be weak.
C. A lack of strong user authentication.
D. The ease of unauthorized access points being added to the system.

When these vulnerabilities are combined with the availability of war driving software such as Netstumbler and Ethereal, the ease of installation and the popularity of the technology, risks arising from a WLAN deployment increase greatly. While generally confined to users seeking to determine what they are able to access, the potential availability of patient information being leaked to the public domain through a non-secure installation of wireless technology is significant. Healthcare systems have increasing come under attack by hackers, many seeing the attacks as performing a public service by calling attention to the lack of security in these systems. [Harrod]

Arising from these concerns are two basic types of attacks, passive and active.

> A. "The passive attack, is an attack in which an unauthorized party gains access to an asset and does not modify its content (i.e., eavesdropping). Passive attacks can be either eavesdropping or traffic analysis (sometimes called traffic flow analysis)." [NISTW, 3-19]
> B. "The active attack is an attack whereby an unauthorized party makes modifications to a message, data stream, or file. It is possible to detect this type of attack but it may not be preventable." [NISTW, 3-20]

The risks associated with the use of wireless technology and the 802.11b standard are the result of one or both of these types of attacks. The consequences of these attacks include, but are not limited to, loss of patient and organizational information, legal and recovery costs, tarnished image, and loss of network service. [NISTW, 3-20]

However, even given the inherent risks to systems, the benefits for many users outweigh the these risks. These benefits include greatly increased user mobility and flexibility. This is especially seen in the clinical areas where users now have the option to take small hand-held or tablet devices to the examination rooms to retrieve information, document care that has been rendered or post new orders for patients in real time.

To enjoy the benefits of these networks, the risk to the practice's patient information need to be lessened. GIAC has taken the following steps to mitigate the potential risks by the deployment this technology.

> A. The wireless system, runs on its own sub-net, and attaches to the network via the Netgear GS516T switch and Cisco 2611 router through the firewall.
> B. The Conmpaq CE hand-helds require network authentication to the PDC over VPN. Becasue the information originates outside the firewall it must be protected until within the secured network.
> C. The 128 bit WEP encryption has been enabled on the access point to prevent wireless eavesdropping by outsiders for all traffic between the hand-helds and the access point.
> D. All access points are controlled by Information Systems (IS) and are set not to broadcast Service Set Identifier (SSID) information. This helps to lessen the visibility of GIAC's network making it a less tempting target for "war driving."

E. The IT support company randomly monitors the WLAN using "war driving" tools to verify the proper implementation and maintenance of the network.
F. MAC filtering is used to help prevent unknown devices from accessing the network.
G. Users are required to authenticate to the network PDC before accessing any of the available applications.

In addition to the WLAN configuration the practice manager daily reviews access logs for the critical systems for suspicious activity that could arise from rogue access to the network.

The primary remaining concern remains the static encryption key used in the WEP protocol. The potential for a hacker to download a large amount of information for decrypting remains. Any additional securing of the WLAN, such as acquiring Cisco's Airnet technology, with dynamic assigned encryption keys is out of the cost range for a physician practice the size of GIAC. An additional concern is the exterior perimeter of the practice. GIAC's offices are housed in an office building with a number of public areas and streets. While securing these areas is not an option, the gain on transmitters has been minimized.

The configuration of the WLAN is felt to be reasonable and demonstrates "due care" for minimizing the risk to patient information.

Risk Two: The unavailability of patient information due to virus/malicious software.

Eighty-five percent of respondents to the CSI/FBI Computer Crime and Security Survey indicated that they had been subject to a virus attack. [CSI] In recent memory, Code Red, Nimda and the Anna K. attacks all represent the prevalence of this menace. Recent attacks to the internet's core systems by the SQL Slammer Worm demonstrate the susceptibility of systems to attack.

The presence of viruses and malicious software is well documented. The necessity of having up to date anti-virus software is critical for protecting the availability of GIAC's patient information. The effects of such an attack run the gambit from rendering the information in GIAC's systems unavailable to the complete destruction of the databases. GIAC has identified two areas of concern for the practice stemming from the unavailability of information due to virus/malicious software attack.

1. GIAC is fully dependent on the Millbrook system for the practice's financial management, claims submission and reimbursement. The unavailability of this information due to virus attack would cause a serious disruption in the financial operations of the practice.

2. The providers have identified the availability of patient information during "off-hours" as a standard of care that is critical to their ability to take call and provide

appropriate patient care. The unavailability of patient information from Logician due to a virus attack would seriously hamper the ability of the on-call providers to meet what has been defined as standard of care.

GIAC has sought to mitigate this risk though a layered defense. The front line of this defense is the Sonic SOHO3 firewall coupled with Sonic's anti-virus service. This has provided the practice with "bi-directional" protection. The firewall performs the initial scans and blocks potential incoming virus laden traffic. Potential executables, zip and scripting files are all stripped before any email is allowed into the network. The Exchange mail server is provided with McAfee GroupShield software to detect and remove viruses being sent into the system. The final layer resides on the individual desktops and Compaq CE hand-helds.

Whenever a PC attempts to send traffic to the Internet through the Sonic firewall, a request for the version of the McAfee VirusScan files is automatically returned to the desktop. If the PC fails to respond, the firewall automatically triggers a transparent response. All users are kept updated with the latest version of anti-virus software before accessing the Internet. [SONIC] This passive update for GIAC users has helped to remove some of the human factor in dealing with the virus risk. For example users are prevented from turning off the anti-virus software, by preventing their access to internet without the client response.

As part of the HIPAA compliance plan, the IT support company has committed to providing updated patches for the GIAC system that are required to prevent vulnerabilities to attack. The company maintains a log of CERT advisories and mitigation steps taken as part of their service to GIAC and other healthcare practices in the area.

Risk Three: Unavailability of Information Due to Poor Backup and Recovery Process

Computer systems will crash, malicious software will have an impact, databases will become corrupted. These and more require that GIAC have a robust backup and recovery (B & R) process. As has been stated the information maintained in the Millbrook and Logician systems are critical to the on-going operation of the practice.

The loss of computing ability or a database either by accident or malicious intent requires that the needed information be restored as soon as possible. The two primary systems that GIAC depends on for its operations are regularly updated by the vendors. Introduction of new code into theses systems has caused occasional unplanned downtimes. While the incidence of these occurrences is relatively low, ability to recover quickly is again critical. A review by the practice and the IT support company determined the following for the primary systems:

> Given the financial system requirements to meet specific time windows for the submission of claims, it was necessary to have this system operational within an eight hour period or one shift in the event of unplanned down time.
> Although GIAC has aspirations to "go paperless", paper patient records are still maintained. This provides the practice with a somewhat larger window to recover the clinical system. However, because the patient schedules, lab interfaces and financial interfaces are part of this system, it would need to be operational within 16 hours or two shifts in the event of unplanned down time.

Having these systems unavailable for any extended period of time would cause disruption in the continuity of patient care and in the financial operations of GIAC. Physician practices operate on a relatively thin financial margin, due to cutbacks in third-party reimbursement. The timely processing and submission of claims is critical to maintaining the financial viability of GIAC.

To mitigate this risk both systems are set to backup their data automatically twice a day. During the lunch hour an incremental backup of all updates for the day is prepared, with a full backup run during the night. The office manager working with the IT support company is responsible for these backups. Tapes are on a five week rotation schedule, allowing for a month of data to be on hand at any one time. The operating system is backed up to tape on a weekly basis, again with a five week rotation. In addition to these jobs, the financial system is backed up on a quarterly basis with a fifteen month rotation and a yearly job that is retained for seven years. The IT support company has a courier service that picks up the tapes every morning and stores them off site at their offices.

Testing the backup and recovery process is a disruptive and costly procedure for the practice. However the administrative procedures required by HIPAA mandate that GIAC have a contingency plans and backup and recovery plans. Without reasonable testing of these plans they become only so much paper. The IT support company now once a year simulates a server crash for each of the primary systems. Testing includes them bringing in a cold server, installing the OS and needed applications and bringing the system on-line for use. This generally occurs over a weekend, with no disruption to the actual working systems.

Assignment Three: Policy Review

Information security policies are necessary in organizations for several reasons. These include regulatory requirements, the definition of accepted behavior and activities in the organization, the establishment of standard operating protocols and a definition of senior management's intent.

The following policy is based on a policy from the author's organization. Given GIAC's dependence on the username/password combination appropriate end user authentication is critical for the preservation of system confidentiality, integrity and availability.

GIAC Healthcare Policy 11.004 **Effective Date: 10/01/2002**

Subj: End User Access Management

Scope: This policy applies to all information systems of GIAC, which access, process or store patient and/or organizational information and to all individuals using those systems, regardless of their relationship with GIAC.

Purpose: To provide guidance for management of user sign-ons to the information systems of GIAC . One of the most serious responsibilities that all employees assume is the patient's right to privacy. This right is mandated by ethical behavior, is required by law and is expected of all GIAC employees.

In the course of performing assigned tasks at GIAC Healthcare it will be necessary to access the GIAC Information Systems. These systems contain both patient and organizational information that is confidential. Access to these systems is based on assigned privileges. The privileges assigned to a user are based on the assigned job tasks of a specific job description developed by the functional area manager (FAM) and approved by GIAC Medical Director.

Users will be assigned a username that is unique for them to access the information systems of GIAC and to perform their assigned job tasks. This username when used with a password to access GIAC information system is the equivalent of their signature. This combination is not to be divulged to anyone. The timely preparation of new employee sign-ons is necessary to prevent the sharing of sign-ons, the use of another employee's sign-on during training and provide for user accountability. Modification of privileges is necessary as roles and job assignments change. Revocation of access upon termination is necessary to prevent the inappropriate access to GIAC systems by either an employee terminated for cause or by an outsider gaining the username/ password combination of a dormant account.

Maintaining the security of a username/password is necessary for the protection of patient and organizational information. Inappropriate access to patient or organizational information risks the loss of our patient's trust, causing potential harm to our patients and places GIAC vulnerable to potential civil and regulatory action.

1. User Access - General Information:

A. The combination of a USERNAME and PASSWORD is used to gain access to the information systems of GIAC and defines the functions that a user is able to perform in the system. This combination is user-unique and is the equivalent of a user's signature.

B. System access consists of two parts, the USERNAME and the PASSWORD The USERNAME consists of six (6) characters.

1) Two character functional area identifier
2) Three character employee initials ("N" will be used where no middle initial is indicated)
3) One character sequence number

Functional area identifiers:

IT Support	IS	Administration	AD
Fiscal Services	FS	Clinical Staff	CS

C. Failure to adhere to this policy will subject the employee to the provisions of the GIAC Healthcare's sanctions policy.

2. Issue of User Access:

A. The Information System Access Request form, will be used when a user sign-on is to be requested. This request is to be filled out by the FAM as part of new hire orientation during the first day of employment and sent to the Office Manager for processing.

B. The USERNAME will be built by the Office Manager. The username will be returned to the requesting manger to be issued to the employee within one (1) day of receiving the request. It is the responsibility of the FAM to ensure the username is provided before training begins for the new employee.

1. The Office Manager will build the username based on the privileges defined in the role matrix, prepared by the FAM and approved by the GIAC Medical Director.
    a. The Office Manager is responsible for reviewing the appropriateness of requested access as it relates to the assigned job duties.
    b.) Any deviation from the approved privilege matrix is to be justified by the requesting FAM and requires the approval of the GIAC Medical Director.

2. All personnel who require access to GIAC systems must successfully complete an approved course of instruction from their FAM before final access is issued. Users will be issued their username by their FAM for use in training. As part of the training the FAM will ensure that the initial password issued with the username is changed.

3. The FAM will ensure that a GIAC Confidentiality Statement is completed by all users before the username is assigned. This statement is a requirement of employment and will be returned to the Office Manager for filing in the user's employment file upon signing.

4. The Office Manager is to monitor the initial change of the user password with the network Event Viewer tool.

E. It is the policy of GIAC not to change Usernames when a user's name or position changes. This is to provide for continuity and accountability of user activity.

Modification of User Access

A. Modifications to user access due to changes in assigned job duties or roles are to be requested by memo by the FAM to the Office Manager.

1. The Office Manager is to review the requested changes and if appropriate make the changes within one (1) working day.
2. Changes that deviate from the approved privilege matrix are to be reviewed and approved by the GIAC Medical Director in writing to the Office Manager.

3. Termination of Access:

A. All users of GIAC who require access to the EMHIE to perform their job assignments will have appropriate access codes assigned to them. The de-activation of this code will occur upon termination of their employment.

1. The FAM is to notify the Office Manager of the termination of any user.
   a. If the termination is for cause, the notification is to take place immediately upon notification of the employee dismissal.
   b. If the termination is at the employee's request, the notification is to take place within one (1) working day.
2. The Office Manager will inactivate the user's accounts.
   a. If the termination is for cause, the inactivation is to take place immediately upon notification by the FAM.
   b. If the termination is at the employee's request, the inactivation is to take place within one (1) working day.

Submitted by: **Date:**

GIAC Office Manager

Approved by: **Date:**

GIAC Medical Director

Review of Policy:

The policy stands on its own. This is a clear concise policy, easily used by a small to medium sized physician office practice for the management of user sign-ons.

1. The purpose of the policy is clear, the management of user sign-ons for the GAIC systems. The introduction provides the background and rationale for the policy, that of protecting the information in the GIAC systems. The importance of maintaining the security of sign-ons is emphasized in light of protecting the interests and information of GIAC and the risks which might arise if the policy is not followed. The username/ password combination for authentication to the systems is critical because, both office and remote access is based on the username/password combination. (Why)

2. The scope of the policy is clearly stated and leaves out no one from this important aspect of system security. The signature of the practice medical director places the authority of the policy with the senior management of GIAC, requiring compliance from all employees.

3. Policy:

A. Reading through policy sections the responsible parties, their responsibilities and processes are defined (Who, What):

1) Functional Area Manager
   a) Requests a user sign-on during the first of hire;
   b) Requests privileges appropriate to the job tasks assigned;
   c) Ensures the user sign-on is built within the required timeframe;
   d) Receives the new user sign-on;
   e) Provides the user sign-on for the employee, ensuring that the password is reset;
   f) Provides training for the employee;
   g) Requests modification to privileges as required by assigned job tasks;
   h) Ensures the confidentiality statement is signed and returned to the Office Manager;
   i) Notifies the Office Manager of employee termination;
   j) Prepares and submits privilege profiles for the functional area.

2) Office Manager

a) Reviews the appropriateness of the request builds the sign-on and provides back the user sign-on within the prescribed timeframe;
b) Monitors the initial password change;
c) Retains the confidentiality statement in the employee file;
d) Reviews the appropriateness of all modification requests;
e) Modifies privileges;
e) Revokes access upon employee termination.

3) GIAC Medical Director
a) Reviews and approves privilege profiles;
b) Approves any access request that deviates from the privilege matrix or changes to the matrix.

4) The employee
a) Provides the personal information for the access request;
b) Maintains the security of their username/password combination;
c) Completes required training;
d) Signs a confidentiality statement.

B. The process for managing the user sign-on is laid out (How). This includes the initial assignment of access, modification of privileges and employee termination.

C. The key events in each process and their and their associated timeline (When) for accomplishment are defined. A system of checks for determining compliance is provided.

D. The reader is referred to another document that is HIPAA required to deal with the failure to follow the policy.

Assignment Four: Develop Security Procedures

GIAC Healthcare Procedure **Effective Date: 10/01/2002**

Subj: System Access Request

Scope: This procedure applies to all information systems of GIAC Healthcare, which access, process or store patient and/or organizational information and to all individuals using those systems, regardless of their relationship with GIAC.

Purpose: To provide for the timely and orderly processing of user access requests for the information systems of GIAC. Access to the GIAC systems will be permitted according to management and process owner approved privileges. This procedure

deals with the requesting of user access to the systems of GHA. To ensure that new employees are assigned a system sign-on in a timely manner this procedure is to be followed for all new hires in the practice. The timely preparation of new employee sign-ons is necessary to prevent the sharing of sign-ons or the use of another employee's sign-on during training. To preserve the confidentiality of the information in the GIAC systems, while ensuring that employees are provided the necessary access for job function, the appropriate privileges must be requested and assigned during this process.

Maintaining the security of a username/password is necessary for the protection of patient and organizational information. Inappropriate access to patient or organizational information risks the loss of patient trust, causing potential harm to patients and places GIAC vulnerable to potential civil and regulatory action.

It is the functional area manager's (FAM) responsibility to request the username from the Office Manager and only request appropriate privileges for the employee's assigned job tasks as defined in their job description.

1. Requesting A User Sign-on:

A. A user sign-on will be requested immediately upon hiring by the functional area manager for any employee that requires access to any GIAC information system in performing their job.

1) The necessary information to complete the request is to be obtained by the FAM during the initial employee orientation.
2) The Office Manager will review the new hire log to ensure that employee usernames are requested within the first day of employment.

B. The Information System Access Request form (ISAR) (attachment #1) will be used for all access requests.

1) Provide the information requested in the header of the ISAR.
    a. If this is a new employee leave the Master Account field blank.
    b. If this request is for additional privileges fill in the employee username in the Master Account field.

2) Check the appropriate systems that are needed to perform assigned job duties.
    a. To access the GIAC Healthcare systems from off-site Remote access should be requested and Section three completed.

3) Section 1 must be completed for all new employees. This section is mandatory for the request to be processed. If the GIAC Enterprise Number is unknown, providing the remainder of the information in this section will allow the assignment of the enterprise number.
4) For an email account is requested Section 2 of the ISAR is to be completed.

a. The computer location and PCID are necessary to allow software support to correctly configure the user Outlook profile.
b. If the user will need to communicate outside the organization via email be sure to request internet/external mail.
c. Indicate the training plan for the user. The mailbox will be inactive until proof of training completion is provided to the Office Manager by the FAM.
d. If proxy or delegated access to folders, calendars, distributions lists and mailboxes are needed indicate the specifics of the request in item 4 of this section.

5) If remote access is needed complete Section 3. The correct indication of home PC operating system is needed to ensure the correct materials and instructions are provided to the user for remote installation.
6) The signed request is to be forwarded to the Office Manager for processing during the initial orientation. A request lacking either the employee or manager signature will be returned to the FAM for completion.

C. The username will be built by the Office Manager and returned to the FAM within one (1) working day of receiving the request.

1) The Office Manager is responsible for reviewing the appropriateness of requested access as it relates to the assigned job duties.
2) Any deviation from the approved access matrix is to be justified by the requesting FAM and requires the signature approval of the GIAC Medical Director.

D. The user sign-on will be issued to the FAM.

1) It is the FAM's responsibility to ensure that the end-user receives the USERNAME as part of the training and orientation program.

E. When sign-ons are assigned to users, they are given their username. The FAM will coordinate the activation of the username and initial password with the Office Manager at the time of initial sign-on for training.

1) The Office Manager will review the network Event Viewer to ensure the password change has taken place.
2) The Office Manager is to monitor new accounts for activity. Any account not activated with three (3) working days of issue is to be inactivated.

Submitted by: **GIAC Office Manager**	**Date:**
Approved by: **GIAC Medical Director**	**Date:**

Attachment #1

GIAC HEALTHCARE
Information Systems Access Request

4 Complete the following. Date of Request:

Name:

First Name Middle Initial Last Name Suffix

Master Account[1] **Complete Section 1 if necessary**

Primary Job: Contact Work Phone Number:

Please check the systems and specify the privileges needed. List any special privileges in "Other"

- ☐ Logician Access
  - ☐ Provider
  - ☐ Provider Support
  - ☐ Patient Records
  - ☐ Patient Billing
- ☐ Network Access
- ☐ Exchange Email
- ☐ Other _____

- ☐ Millbrook
  - ☐ Provider
  - ☐ Provider Support
  - ☐ Patient Records
  - ☐ Patient Billing
- ☐ Remote Access
- ☐ Administrative Access

I agree to adhere to all GIAC policies and procedures dealing with Information Integrity and Security and understand that it is my responsibility to become familiar with the Information and Security policies and procedures.

_____ _____

Employee Signature Date Functional Area Manager Date

SECTION 1 REQUEST FOR MASTER ACCOUNT

The IT Support Help Desk will use this information to confirm your identity when resolving issues. All information will be maintained as confidential by the staff.

4 **GIAC Enterprise Number**: _____

_____

Previous or Maiden Name Gender (Male/Female)

_____

Street Address Apt #

_____

City/Town State Zip

Date of Birth: _____ Place of Birth: _____

(Month Day Year) (City, State/Province, Country)

[1] We use the Master Account (previously known as XXXXX ID) to provide a consistent login name throughout GIAC. All account requests need a Master Account. Your Master Account will have the following pattern XXYour Initials# (ISABC1, PPXYZ1, etc.) If you need a Master Account complete Section 1.

SECTION 2 REQUEST FOR OUTLOOK-ENTERPRISE EMAIL

Items 1, 2, and 3 in this section are required.

1. Do you: ☐ Need a new computer or ☐ Have an existing computer

_____ _____
Location of Computer PC ID (AHOSP-xxx, 936-xxx, etc.)

Is this computer shared with other users? ☐ Yes ☐ No

2. Is Internet mail (external mail) required for business use? ☐ Yes ☐ No

3. Training plan: ☐ Attending Class _____ ☐ Other _____
(date if known) (please specify)

4. Special Requests (Delegate Access for Calendars and Mailboxes, Distribution Lists, etc.)

_____

4 If possible please provide the following information about your computer. Otherwise leave blank and Network Services will determine if the computer is adequate for e-mail and network ready.

Hardware Information
Enter Model Here
_____
Make

Enter Memory Here ☐ Yes ☐No
_____
Memory (RAM) Free Disk Space Network Connection

SECTION 3 REQUEST FOR REMOTE ACCESS

(REMOTE AND ROAMING ACCESS TO EMAIL)

Remote Privileges are used to provide remote and roaming access to e-mail (Outlook), Logician and other services. See instructions for details.

_____ _____
Location of Computer PC ID (AHOSP-xxx, 136-xxx, etc.)

_____ _____
Location of Computer PC ID (AHOSP-xxx, 136-xxx, etc.)

Do you need diskettes/CD and instructions for home installation? ☐ Yes ☐ No
☐ CD ☐ Diskettes

If yes, operating system requirements:
☐ Win95/98/NT/2000 ☐ MAC
Send diskettes to:

_____
Department Office #

_____
Site

Bibliography:

Anderson, Kurt, Technical Reference, Author's organization.

Avolio, Fred, "The Real Deal on Wireless", Information Security Magazine, August 2002, http://www.infosecuritymag.com/2002/aug/justthebasics.shtml

Clark, Bill and Bresee, Jim, " Secure Internet Access to Patient Information", Journal of the Healthcare Information and Management Systems Society, Vol. 12, Number 1, San Francisco, CA, 1998.

Cisco Systems, "Configuring the Cisco Wireless Suite", Revision 2.0, http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wrsec_an.htm , retrieved 22 October 2002.

Computer Security Institute, "CSI/FBI Computer Crime and Security Survey", 7 April 2002, www.gocsi.com/press/20020407.html

Duffy, Daintry, "How to Rope In Rowdy Technologies", CSO, Vol. 1, Number 2, October 2002.

Ford, John, "GIAC Enterprises Security Management for Non-Profit Health Care Providers", SANS – Information Security Officer GISO- Basic Practical Assignment Version 1.1, retrieved 22 January 2003.

General Electric Medical Systems, "Information Technologies" http://www.medscapeinc.com/products/logician/ , retrieved 21 January 2003.

Gue, D'Arcy, "HIPAA Advisory, Phoenix Healthcare Systems, retrieved 12 October 2002, http://www.hipaadvisory.com/regs/securityoverview.htm

Harrod, Bill and Marne Gordan, "HIPAA Incident Response Essentials – The Eight Daily Minimum Requirements", TruSecure Web Presentation, January 31, 2003.

Krause, Micki and Tipton, Harold, editors, Handbook of Information Security Management 1999, Auerbach, Boca Raton, FL, 1999.

"Wireless Security: Meeting the Threats, Summary Chart", Information Security Magazine, http://www.infosecuritymag.com/archives2002.shtml#jan, January 2002.

McAfee, "Product Information", http://www.mcafee.com/myapps/default.asp, retrieved 28 January 2003.

Millbrook Practice Management Systems, "Product Overview" http://www.millbrook.com/products_01.asp , retrieved 21 January 2003.

Mission Statement from the author's organization

National Institute of Standards and Technology (NIST), Risk Management Guide for Information Technology System, Special Publication 800-30, October 2001.

National Institute of Standards and Technology (NISTW), Wireless Network Security, 802.11, Bluetooth and Handheld Devices, Special Publication 800-48, November 2002.

National Research Council (NRC), Committee on Maintaining Privacy and Security in Health Care Applications, For the Record, Protecting Electronic Health Information, National Academy Press, Washington, DC, 1997.

SonicWall, "Firewall/VPN Appliances", http://www.sonicwall.com/products/vpnapp.html retrieved, 22 January 2003.

Tippet, Peter, "Wireless Security – A Contradiction in Terms", TruSecure Web Presentation, November 11, 2002.

Wood, Charles, "The Human Firewall Manifesto", Computer Security Journal, Vol. 18, Number 1, San Francisco, CA, Winter 2002.

Wood, Charles, Information Security Policies Made Easy, Version 6, Sausalito, CA, 1997.

Zeltser, Lenny, "Separating Resources on Real World Network", SANS Beyond Firewalls Conference, Denver, CO, August 2002.