GIAC Health System of the Commonwealth's

Information Systems Top Security Risks

Temptation usually comes in through a door that has deliberately been left open.

- *Arnold H. Glasow*

GIAC – GISO BASIC

Practical Assignment

V 1.2

Robert W. Hodges

Abstract

This paper deals with a fictitious healthcare company called GIAC Health System of the Commonwealth. The overall project involved identifying three top information systems risks to GIAC Health System of the Commonwealth and to develop an appropriate security policy and procedure to mitigate the top risk to the “crown jewels” of the company.

Table of Contents

Illustrations

Description of GIAC Health System of the Commonwealth

GIAC Health System of the Commonwealth (GHSC) is one of ten local systems of the larger GIAC Health System Inc. (GHSI) which all are not-for-profit healthcare organizations. The GHSC local system is made up of three owned or joint ventured main acute care hospitals, two long-term or nursing care facilities, along with numerous primary care clinics, outpatient facilities, home health care services, and hospices with approximately four thousand employees total.

Within each of the hospitals, there are roughly seventy-five departments. Most of these departments are duplicative of the other hospitals. Typically there are the core clinical departments (healthcare givers) such as Laboratory, Radiology, Nursing, Labor and Delivery, Nursery, Emergency, Intensive Care, Surgery, and Occupational Medicine, Primary Care, Home Health Care, Hospices, and outpatient facilities. There are also non-clinical or ancillary support departments such as Information Systems, Medical Records, Finance, Payroll, Human Resources, Plant Maintenance, Housekeeping, and Safety and Security.

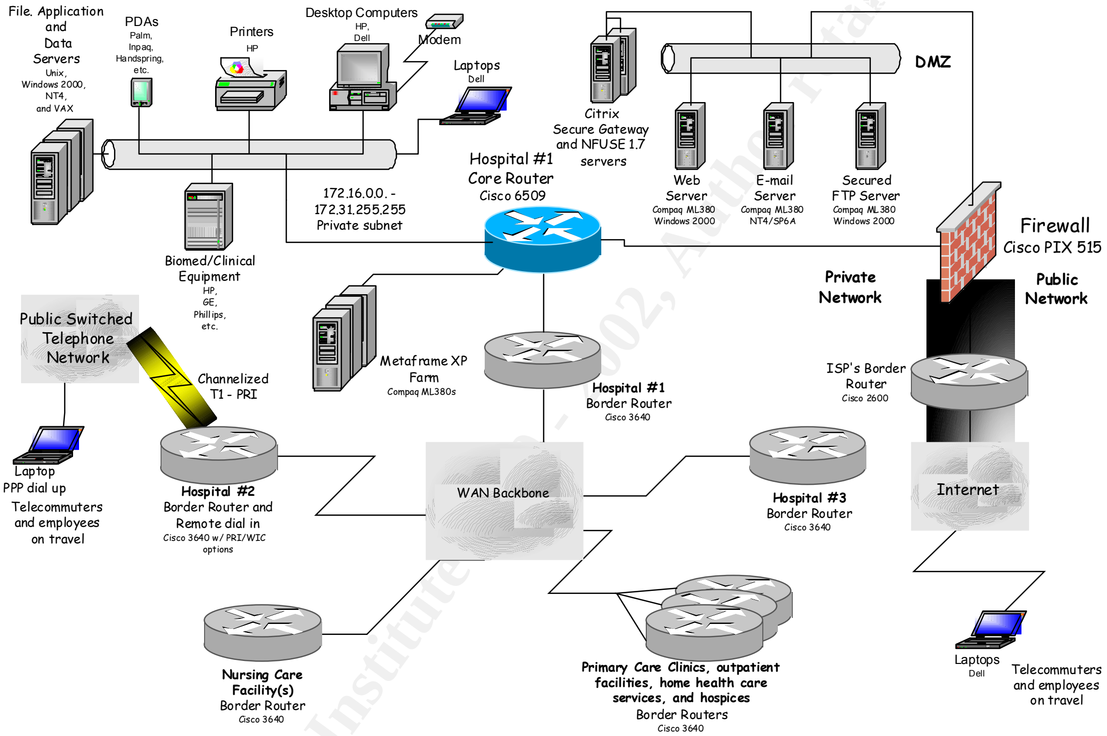
The business office and materials management have been centralized to a single location in order to enjoy the economies of scale it provides. Their applications reside on servers located in the same hospital they are located in which aids in their response time, lessens the WAN and remote bandwidth needs, and helps in case of a business continuity or disaster recovery situation.

There are thirty-five information systems employees to support the local system. There are ten information support analysts and a complement of three senior technicians, six level-two technicians, and six level-one technicians. There are also three customer service representatives that man the local system's helpdesk or call center, and ten telecommunications operators that man the switchboards.

The management positions include four directors - the Director of Networks and Technologies, the Director of Application Support and the Director of Project Management and the Director of Telecommunications. There is also an Information Security Officer. All of which report to the Chief Information Officer to who answers to the Chief Financial Officer of the local system.

GIAC Health System of the Commonwealth's IT Infrastructure

Figure 1 – GHSC's IT Infrastructure


File. Application and Data Servers
Unix, Windows 2000, NT4, and VAX
PDAs
Palm, Inpaq, Handspring, etc.
Printers
HP
Desktop Computers
HP, Dell
Modem
Laptops
Dell
Biomed/Clinical Equipment
HP, GE, Phillips, etc.
172.16.0.0. - 172.31.255.255 Private subnet
Hospital #1 Core Router
Cisco 6509
Citrix Secure Gateway and NFUSE 1.7 servers
DMZ
Web Server
Compaq ML380 Windows 2000
E-mail Server
Compaq ML380 NT4/SP6A
Secured FTP Server
Compaq ML 380 Windows 2000
Firewall
Cisco PIX 515
Private Network
Public Network
Public Switched Telephone Network
Channelized T1 - PRI
Metaframe XP Farm
Compaq ML380s
Hospital #1
Border Router
Cisco 3640
ISP's Border Router
Cisco 2600
Laptop
PPP dial up
Telecommuters and employees on travel
Hospital #2
Border Router and Remote dial in
Cisco 3640 w/ PRI/WIC options
WAN Backbone
Hospital #3
Border Router
Cisco 3640
Internet
Nursing Care Facility(s)
Border Router
Cisco 3640
Primary Care Clinics, outpatient facilities, home health care services, and hospices
Border Routers
Cisco 3640
Laptops
Dell
Telecommuters and employees on travel

The GIAC Health System of the Commonwealth's IT Infrastructure goal is to support local healthcare. Protected Health Information (PHI) above all, makes the fundamental informa tion security tenets of confidentiality, integrity and availability even more poignant; as there are literally lives at stake.

Please refer Figure 1 – GHSC's IT Infrastructure. There are three hospitals in the lo cal system. Hospital #1 serves as the Network Operations Center (NOC) for most applications. The trend is to move most, if not all core services to Hospital #1 eventually. Hospital #2 serves as the remote dial -in point of presence via its closeness to the central office of the local telephone provider, which mitigates costs. The dial-in connection is provisioned as PRI line and therefore can accept both 56Kbs and ISDN connections, which also allows multilinkin g capabilities. The remote dial -in set-up is primarily for the use of Information Systems personnel and a number of support vendors. Network access authorization is handled through Challenged Handshake Authorization Protocol (CHAP) and strict utilization of Access Control Lists (ACL) on the dial-in border router. The dial-in client can then access a Citrix session or PCAnywhere to their desktop if applicable.

The WAN backbone is provisioned at 100Mbs full duplex ATM between hospitals. The other locations are tied into the WAN cloud with various levels of guaranteed throughput via the same common provider. For most remote users, a secure connection via a Citrix – NFUSE (Figure 2 – NFUSE – Citrix Solution) solution via the Internet is provided.

All three hospitals use Cisco as a standard for all routers and switches. The Cisco 6509 is at the heart of all three hospitals specific infrastructures.

An Intruder Detection System (IDS) has been purchased, but not implemented as of yet.

The file, application, data and biomedical/clinical servers shown are the heart of the HIS. As per the corporate-wide standard, Compaq manufactures them all. These servers are where the PHI, financial, and otherwise confidential data is created, used and stored. Therefore, the local and remote users access these servers the most. All company desktops are either Hewlett Packard or Dell and all laptops are Dell.

Novell Directory Services is utilized with the administration of Microsoft users through Novell Account Management and Novell's Console One products.

The Demilitarized Zone (DMZ) Network is separated from both the Public Network (ISP side) and the Private (internal) Network by a firewall. The Private (internal) Network is protected from the DMZ and Public networks. There is also an extra protection layer by way of the Internet Service Provider's (ISP) border router.

Desktops, PDAs, and indirect interfacing between disparate systems are how the data is derived and received. Of course printers are available for output.

The Web server located in the DMZ houses GHSC's intranet and Internet sites. The intranet site is home for employee reference such as telephone listings, policies and procedures, what's happening in GHSC, and links to sister hospitals and the corporate Internet site. The Internet site is also for employees with an addition of the NFUSE – Citrix connection as an option for access to the internal network via the Internet.

GHSC's email server is located in the DMZ to keep malicious attacks from entering the internal network via email vulnerabilities. Also located in the DMZ is the secured FTP server. This is a safe haven for file transfer drop-offs and pick-ups from and to supporting vendors. As part of the defense in depth strategy, this is as far as the vendor is allowed, which adds a layer of protection to security of the internal network.

Business Operations

GIAC Health System of the Commonwealth's intrinsic business flow of healthcare is committed to patient care. In it's analog form, patient care itself has a countless number of processes. Each of these processes must be factored into electronic data algorithms to aid in the decision-making that drives the healthcare process itself. Other functions include electronic documentation, auditing, and ancillary support, e.g., Payroll, Human Resources, Materials Management, etc.

Due to a myriad of accreditation consortiums, federal, state and local regulations, and in particular the Health Insurance Portability and Accountability Act of 1996 (HIPAA), GHSC must adhere to the utmost scrutiny dealing with PHI that is possible.

The key business operations that deal with the highest information security constraints are clearly patient information related, for example, the Medical Records and Finance departments. A medical record includes PHI, i.e., patient demographics, diagnosis, medical history, etc. A financial record includes PHI, i.e., patient demographics, credit information, insurance information, etc.

Most clinical departments share basic business and data flow demands of placing orders, receiving results and posting charges. These are the same basic demands that are typically accessed by remote means from physicians' offices, outpatient clinics, and other healthcare giver entities.

Remote access is needed to support both clinical and non-clinical applications. For the clinical users, the application(s) that is most accessed and therefore most at risk is the hospital's HIS system. Within this all-encompassing application are modules or sub-applications. Each of these modules corresponds to a clinical or non-clinical department as mentioned above.

As a clinical example, the local system's laboratories, one at each main hospital, completely rely on the laboratory module in the HIS for its data flow, which in turn supports its business flow. This is true for any and each clinical application.

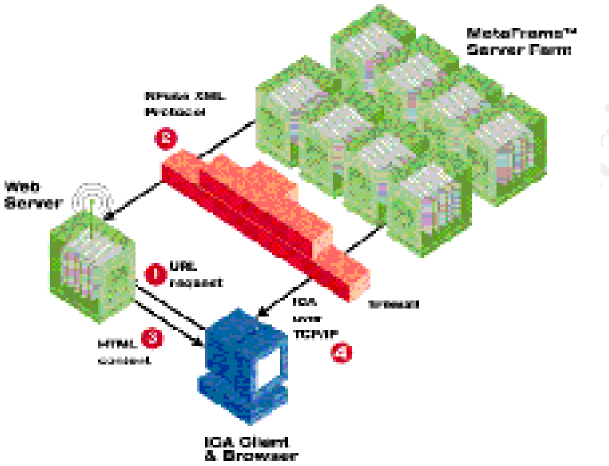
To illustrate a typical clinical process - A doctor orders a laboratory test to be carried out by the use of paper script. In turn, a nurse places the order on a convenient personal c omputer to have certain tests completed on a patient's blood or urine for example. The access route to the Laboratory server, depending on the location can take different routes. These routes could be within the same hospital, across the WAN from a diffe rent hospital, remote dial -in and across the WAN or through the Citrix solution to the server. These tests then produce results through subsequent processing that eventually get posted to the patient's electronic record, to the printer at the patient's nurses station, and to electronic display for the doctor, nurse or other caregiver to continue with providing healthcare to the patient. Also, billing charges for these tests utilize the financial module in the same HIS for subsequent billing to the patient's insurance company or directly to the patient via internal interfacing means.

For the non -clinical users, the top accessed applications would be information systems related, e.g., network administrators, an alysts, and on-call technicians would access routers, servers, application administrative programs, and those wanting to remotely access their corporate email, especially during employee travel. The methods for remote access are the dial -in and Internet.

More and more, the Internet is becoming the transport medium of choice. Internet access is already required for some processes like insurance verification and some state patient (de -identified) database access. It is safe to presume that most clinics, h ealthcare entities, insurance companies, and regulator entities will have Internet connections, if not already; consequently the obvious trend is the inevitable requirement to go paperless. This added need as a result, will require the key service of heal thcare information to be the secured Internet path for all PHI with a dial -in solution as a backup.

As mentioned, within the Health Information System (HIS) umbrella application(s) are specifically designed sub -applications. Access to these sub-applications, file transference and access to pertinent documentation are the needs the use of remote access or to and from outside entities. This is where the use of a Citrix – NFUSE - Metaframe solution became the heart of the remote access approach.

Figure 2 – NFUSE – Citrix Solution



For the time being, there is a myri ad of companies sending and receiving PHI to a secured FTP server located in the Demilitarized Zone (DMZ) via direct dial -in through Hospital #2's border router or via the Internet NFUSE solution.

As Figure 1 – GHSC's IT Infrastructure shows, the telecommuters and employees on travel can either dial -in directly or access the internal network via the Interne t.

In the past, the vendors, in order to pick up and deliver pertinent files or access the appropriate equipment for support issues historically had a modem attached to their specified equipment for them to access. Security usually consisted of questionable set-ups involving remote access via products like PCAnywhere, Blast, CoSession, etc.

Identification of the Three Most Critical Risks

Protected Health Information (PHI) and confidential business data, which exist on the internal network, are the “crown jewels” of GIAC Health System of the Commonwealth, and as such the mitigation of the exploitation of this data by various means is key. This would include inside (private internal network) and outside (public external network) influences. Therefore, all three GHSC’s top risks fall in a general category of remote access.

There are general penalties to be levied for improper disclosure of (PHI) especially as described in the HIPAA regulations stipulate penalties of to $100 for each such violation, with a total amount imposed for all violations may not exceed $25,000 per calendar year. [i] Specifically, any wrongful disclosure of Protected Health Information a person can be fined up to $50,000, imprisoned up to one year, or both; if the offense is committed under false pretenses, be fined up to $100,000, imprisoned up to 5 years, or both; and if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined up to $250,000, imprisoned up to 10 years, or both. [ii]

The top three risk areas to PHI and confidential data are:

Risk 1: Unauthorized Sniffing on WAN segment.

As seen in Figure 1 – GHSC’s IT Infrastructure, the WAN backbone is represented by a cloud because it is a particularly ethereal method of connecting all facilities through a third party network. The threat of active sniffing of GHSC’s WAN data outside of the jurisdiction of GHSC is very possible. The third party’s technical staff definitely has the means for sniffing the WAN and possible due to mistakes in provisioning, someone else may be on the same WAN segment. The vulnerability lies is in the fact that the methodology in place currently is inherently not secure as the data transporting through the WAN is being passed in the clear. GHSC is putting undue demands on the vendor to keep GHSC's data secure. In general, vendors are unwilling to tran sfer the risk to themselves. Therefore, it is the responsibility of GHSC to secure the data before "handing" it over to the WAN service.

The concern to GHSC is that PHI and confidential data are at risk of being exploited by improper disclosure. This type of disclosure would have a negative impact on business due to negative publicity and loss of customer confidence as there could be real life threatening issues. The last thing GHSC wants to see is a headline about an improper PHI disclosure on the front page of the local newspaper. It would also have a financial impact directly due to fines levied by the federal HIPAA regulations a nd probable lawsuits. In due course, there could also be GHSC personnel possibly being incarcerated.

To mitigate this risk GHSC should use a method of encryption, e.g., AES, 3DES, etc., involving all data leaving each site. Also, a firewall should be put into place at each sites' demarcation point with the WAN. This would thwart attacks from the WAN. These two methods together would give a reasonable defense in depth strategy comfort level, for even if the WAN had active sniffing on it, there would be little danger of unauthorized disclosure of PHI or confidential data.

Risk 2: Unauthorized Access to Protected Health Information on portable computers.

The threat is someone other than the owner could have access to the PHI or confidential data. It could be innocuous or deliberate it doesn't matter. Someone's child may do his or her homework on the same laptop or home PC that their parent uses to access patient and financial data during the day.

Another scenario could be a laptop on the kitchen table of a telecommuting medical record's transcriptionist left on a screen that reveals some basics of patient data, e.g., patient's name and the date of a pending clinical procedure, to only have a neighbor come over for coffee and happen to read it, they recognize the patient and tell their friends and they . . . etc.

The vulnerability is the fact that PHI and confidential data resides outside the physical or logical walls, therefore out of the immediate control of GHSC. This has transferred the majority of the risk to the end user.

Once more, the concern to GHSC is that PHI and confidential data are at risk of being exploited by improper disclosure. This type of disclosure would have a negative impact on business due to negative publicity and loss of customer confidence as there could be real life threatening issues. It would also have a financial impact directly due to fines levied by the federal HIPAA regulations and probable lawsuits. In due course, there could also be GHSC personnel possibly being incarcerated.

Mitigation of this risk would lie in the education of the portable computer users. The users need to be aware of privacy and security issues, social engineering ploys, and company policies and the sanctions that go with them.

Risk 3: Unauthorized Remote Access via Attached Modems within the Internal Network.

This, by far, is the greatest risk to the "crown jewels". All of the applied detective work is for naught, no matter how good the security is at the "front door", if there is a wide -open "back door", there is, in effect, no security. Even if there is only one rogue or unsecured modem on the private internal network, there constitutes a security breach, which could result electronic disclosure of Protected Health Information (PHI), which would result in making GIAC Health System of the Commonwealth responsible in a court of law. This in turn would have a negative impact on business due to negative publicity and loss of customer confidence as there could be real life threatening issues. It would also have a financial impact directly due to fines levied by the federal HIPAA regulations. In due course, there could also be GHSC personnel possibly being incarcerated.

The inherent vulnerability is there is a "back door" of which to gain access to the private internal network where Protected Health Information (PHI) and confidential data is kept. This vulnerability is manifested by way of the existence of modems still on various personal computers is largely, if not totally, due to legacy systems. These legacy systems are a product of evolution, out-dated management styles, and prior, less strict regulations over the years. Some of these modems are dial-out only, which may seem on the surface more secure than their counterpart the dial-in capable modems. Yet, the threat is still existent either way, two-way data transfers can be accomplished no matter whom makes the initial connection. Also, callback mechanisms can be manipulated to render them unsecured. Simply, these "back door" connections circumvent the firewall and its intrinsic securities.

In short, the mere existence of these modems jeopardizes the security of the network, thereby inevitably letting it potentially happen again and putting PHI in unceasing peril.

The threat is that any "Script Kiddie" leveled hacker and above can run a "War Dialer" on the network and find the vulnerable modems on the private internal network. Not only is internal PHI and confidential data in jeopardy, the intruder can now look like an employee to further social engineer security breaches or create havoc by impersonating an employee to the outside as the inherent address will be from the inside of the private internal network.

To reduce this vulnerability all modems must be done away with. Through policy reform, standards, procedures and guidelines should all be of one accord. If the risk analysis allows, it would minimally require that callback features be enabled, and/or the modem must be powered off and disconnected from the phone system except during that time that a connection is required. Taking these steps are not foolproof solutions and can only reduce and not totally remove the vulnerability.

To reduce the threats don't publish the modem telephone numbers in the company directory. If a PBX is used, have the internal modems be given phantom numbers so they cannot be dialed into from the outside or call route to where they do not accept calls in at all. Instead, utilize a remote dial-in solution such as a Cisco router with dial-in capabilities and the inherent securities built in or move these services to an Internet solution where the "front door" is capable of handling the proper security. Running awareness programs, establishing policies and enforcing sanctions as prescribed, can also lead to reducing this risk.

The Evaluation and Development of a Security Policy

The following exemplar policy was obtained from http://www.sans.org/newlook/resources/policies/Remote_Access_Policy.doc.[iii]

Remote Access Policy

1.0 Purpose

The purpose of this policy is to define standards for connecting to <Company Name>'s network from any host. These standards are designed to minimize the potential exposure to <Company Name> from damages which may result from unauthorized use of <Company Name> resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical <Company Name> internal systems, etc.

2.0 Scope

This policy applies to all <Company Name> employees, contractors, vendors and agents with a <Company Name>-owned or personally-owned computer or workstation used to connect to the

<Company Name> network. This policy applies to remote access connections used to do work on behalf of

<Company Name>, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

3.0 Policy

3.1 General

1. It is the responsibility of <Company Name> employees, contractors, vendors and agents with remote access privileges to <Company Name>'s corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to <Company Name>.

2. General access to the Internet for recreational use by immediate household members through the <Company Name> Network on personal computers is permitted for employees that have flat-rate services. The <Company Name> employee is responsible to ensure the family member does not violate any <Company Name> policies, does not perform illegal activities, and does not use the access for outside business interests. The <Company Name> employee bears responsibility for the consequences should the access be misused.

3. Please review the following policies for details of protecting information when accessing the corporate network via remote access methods, and acceptable use of <Company Name>'s network:

    a. *Acceptable Encryption Policy*

    b. *Virtual Private Network (VPN) Policy*

    c. *Wireless Communications Policy*

    d. *Acceptable Use Policy*

4. For additional information regarding <Company Name>'s remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

3.2 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.

2. At no time should any <Company Name> employee provide their login or email password to anyone, not even family members.

3. <Company Name> employees and contractors with remote access privileges must ensure that their <Company Name>-owned or personal computer or workstation, which is remotely connected to <Company Name>'s corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

4. <Company Name> employees and contractors with remote access privileges to <Company Name>'s corporate network must not use non-<Company Name> email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct <Company Name> business, thereby ensuring that official business is never confused with personal business.

5. Routers for dedicated ISDN lines configured for access to the <Company Name> network must meet minimum authentication requirements of CHAP.

6. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

7. Frame Relay must meet minimum authentication requirements of DLCI standards.

8. Non-standard hardware configurations must be approved by Remote Access Services, and InfoSec must approve security configurations for access to hardware.

9. All hosts that are connected to <Company Name> internal networks via remote access technologies must use the most up-to-date anti-virus software (place url to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.

10. Personal equipment that is used to connect to <Company Name>'s networks must meet the requirements of <Company Name>-owned equipment for remote access.

11. Organizations or individuals who wish to implement non-standard Remote Access solutions to the <Company Name> production network must obtain prior approval from Remote Access Services and InfoSec.

4.0 Enforcement

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

5.0 Definitions

Term **Definition**

Cable Modem Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.

CHAP Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCIData Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.

Dial-in Modem A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.

Dual Homing Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a <Company Name>-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into <Company Name> and an ISP, depending on packet destination.

DSL Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

Frame Relay A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.

ISDN There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.

Remote Access Any access to <Company Name>'s corporate network through a non-<Company Name> controlled network, device, or medium.

Split-tunneling Simultaneous direct access to a non-<Company Name> network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into <Company Name>'s corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

6.0 Revision History

Critique of Template Policy

The previous policy is very good overall, very succinct and clear.

The purpose is clearly stated as to define standards for connecting to the network from any host. The issue here is to mitigate damages to internal systems and the data residing on it.

The scope is well defined to the extent that it applies to all employees, contractors, vendors and agents with a company-owned or personally owned computer or workstation used to connect to the network and remote access connections, including reading or sending email and viewing intranet web resources. It covers remote access implementations, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc. as examples. It puts in a caveat that this recommended list is not all-inclusive. Yet, it does not cover systems that are on-site but not owned by the company.

The policy section defines the responsibilities of the remote connection; this pragmatic approach to allow general Internet usage as later it disallows split -tunneling or dual homing, which would have created a mutually exclusive situation. It references other related policies. It leads to action by referring to other applicable sites. The addition of hyperlinks would have made it easier for the reader

The policy also defines requirements for access control and other security related information. It defines minimum requirements for network hardware, antiviral software, and the minimum remote computer's specifications.

The responsibility of this policy appears to lie with the Remote Access Services and InfoSec .

There is no effective date mentioned; however actions are specifically designated, such as the enforcement of the policy.

Definitions are included to help in the reader's comprehension and to increase the likelihood of compliance.

Revision of Template Policy

The revised policy as it applies to GIAC Health System of the Commonwealth is as follows:

GIAC Health System of the Commonwealth

Information Systems Policy

Deleted: ¶

Topic:	**Remote Access Policy**	**Policy No.:** ***12345***	**Effective Date:** ***1/17/2005***	
			Revision Date:	
Area:	**Information Services**	**Page 1 of** ***7***	**Approved By:**	**V.P./CIO, Information Systems**

Remote Access Policy

1.0 Purpose

The purpose of this policy is to define standards for connecting to GIAC Healt h System of the Commonwealth 's network to and from any outside host. These standards are designed to minimize the potential exposure to GIAC Health System of the Commonwealth from damages, which may result from unauthorized use of GIAC Health System of t he Commonwealth resources. Damages include the loss or wrongful disclosure Protected Health Information, sensitive or company confidential data, intellectual property, damage to public image, damage to critical GIAC Health System of the Commonwealth inter nal systems, etc.

2.0 Scope

This policy applies to all GIAC Health System of the Commonwealth employees, contractors, vendors and agents with a GIAC Health System of the Commonwealth owned or personally owned computer or workstation used to connect to the GIAC Health System of the Commonwealth network. This policy also covers any computer and communications devices or systems that are present on GIAC Health System of the Commonwealth premises, but which may not be owned or operated by GIAC Health System o f the Commonwealth. This policy applies to remote access connections used to do work on behalf of GIAC Health System of the Commonwealth, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-up modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

3.0 Policy

3.1 General

It is the responsibility of GIAC Health System of the Commonwealth employees, contractors, vendors and agents with remote access privileges to GIAC Health System of the Commonwealth 's corporate network to ensure that their remote access connection is given the same consideration as the user's on -site connection to GIAC Health System of the Commonwealth.

An appropriate departmental manager with the level of Director or above along with the consent of the Director of Networks and Technologies must approve access to or from remote locations to GHSC's corporate network and thereby protecting the electronic assets within.

Audit trail logs of all inbound and outbound access to GHSC's internal network by systems outside shall be maintained. Systems administrators shall regularly review these logs, or u se automated intrusion detection systems to inform them of suspicious activity.

General access to the Internet for recreational use by immediate household members through the GIAC Health System of the Commonwealth Network on personal computers is permitted for all remote access authorized employees. The GHSC employee is responsible to ensure the family member does not violate any GHSC policies, such as not performing illegal activities, and not using the access for outside business interests (Acceptable Use Policy). The GIAC Health System of the Commonwealth employee bears sole responsibility for the consequences if the access is misused.

The following GHSC policies a re pertinent to protect information when the corporate network is accessed via remote access methods, and acceptable use of GIAC Health System of the Commonwealth 's network:

a. Acceptable Use Policy

b. Acceptable Encryption Policy

c. Virtual Private Network (VPN) Policy

d. Wireless Communications Policy

For additional information regarding GIAC Health Syst em of the Commonwealth's remote access connection options, including how to order or disconnect service, troubleshooting, etc., please access the Remote Access Services website.

3.2 Requ irements

There shall be a security -warning banner posted upon initiating access to any GHSC's network. This banner will be compliant to NIH's standard (NIH Warning Banner).

Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see GHSC's Password Policy.

At no time should any GIAC Health System of the Commonwealth employee provide his or her login or email password to anyone, not even family members, see GHSC's Password Policy.

GIAC Health System of the Commonwealth employees and contractors with remote access privileges must ensure that their GIAC Health System of the Commonwealth-owned or personal computer or workstation, which is remotely connected to GIAC Health System of the Commonwealth's corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

It shall not be permitted to let any GHSC personal computer, workstation or other piece of equipment to be connected to any other network while connected to GHSC's corporate network and at the same time. Any need for such service must be addressed by accessing the Remote Access Services website.

Reconfiguration of a corporate or home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

GIAC Health System of the Commonwealth employees and contractors with remote access privileges to GIAC Health System of the Commonwealth's corporate network must not use non-GIAC Health System of the Commonwealth email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct GIAC Health System of the Commonwealth business, thereby ensuring that official business is never confused with personal business.

All hosts that are connected to GIAC Health System of the Commonwealth internal networks via remote access technologies must use the most up-to-date anti-virus software (Antivirus

Guidelines) this includes personal computers. Third party connections must comply with requirements as stated in the Third Party Agreement .

Personal equipment that is used to connect to GIAC Health System of the Commonwealth 's networks must meet the requirements of GIAC Health System of the Commonwealth -owned equipment for remote access .

All GHSC owned equipment will be an agree to permit periodic inspections of GHSC IT equipment and software the employee is using to ensure proper maintenance (e.g., to install software updates and security patches).

The Remote Access Services Team must approve non -standard hardware configurations, and Information Security Officer must approve security configurations for access to hardware. Therefore, organizations or individuals who wish to implement non -standard Remote Access solutions to the GIAC Health System of the Commonwealth production network must obtain prior approval from Remote Access Services Team and the Information Security Officer .

Routers for dedicated ISDN lines configured for access to the GIAC Health System of the Commonwealth network must meet minimum authentication requirements of CHAP.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Please see applicable GHSC's Human Resources policies.

5.0 Definitions

Cable Modem - Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.

CHAP - Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCI Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.

Dial-up Modem - A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.

Dual Homing - Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Corporate network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a GIAC Health System of the Commonwealth-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into GIAC Health System of the Commonwealth and an ISP, depending on packet destination.

DSL - Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

Frame Relay - A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.

ISDN - There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.

NIH – The National Institute of Health.

Remote Access - Any access to GIAC Health System of the Commonwealth 's corporate network through a non -GIAC Health System of the Co mmonwealth controlled network, device, or medium.

Split-tunneling - Simultaneous direct access to a non -GIAC Health System of the Commonwealth network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connecte d into GIAC Health System of the Commonwealth 's corporate network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

6.0 Revision History

Remote Access Security Procedure

Deleted: ¶

Topic:	Remote Access Procedure		Effective Date: *1/17/2005*
	Implementation of the Security-warning banner to Windows NT/2000 and Windows 9X computers on GHSC's network.	No.: *12345* Applicable Policy No.: *12345*	Revision Date:
Area:	Information Services	Page 1 of 6	Approved By: V.P./CIO, Information Systems

Implementation of the Security-warning Banner to Windows NT/2000 and Windows 9X Computers on GHSC's network.

This set of registry modifications cause a dialog box to display the required warning each time a user starts up Windows or logs off and then back on. After the registry entry is made, the warning notification appears even if the personal computer isn't attached to the network or if user doesn't log in to the network.

As mandated in GHSC's Remote Access Policy No.: 12345 under the requirements section, "There shall be a security-warning banner posted upon initiating access to any GHSC's network. This banner will be compliant to NIH's standard (NIH Warning Banner).", this document holds the procedure to carry this out in a uniform manner.

It will be the responsibility of GHSC's Information Technology group to apply this procedure to all computers as stated in the scope section in GHSC's Remote Access Policy No.: 12345.

Auditing of the procedure will be handled through either provided logs from Novell's Zenworks, or in the case of semi-manual registry merges or manual registry edits - a project database will be created and maintained until it is verified that all GHSC's computers have been completed. The Information Technology staff when possible will do spot check auditing during maintenance of said equipment.

This procedure will here forward be integrated into the standard set-up instructions for all computers in GHSC.

Implementation by using Novell's Zenworks for Desktops: [iv]

Create a NAL Object and associated it to all users

Set it to force run

Set the Version to today's date (example 09012002)

(If dealing with Windows 2000 or NT go to step 6., otherwise)

For Windows 9x:

Set OS version equal or greater to Windows 95/98

Add the following to the system registry:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Winlogon]
"LegalNoticeCaption"=" Warning Notice! "
"LegalNoticeText"=" This is a GIAC Healthcare computer system, which may be accessed and used only for authorized GIAC
```

Healthcare Systems' business by authorized personnel. All information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Acces s or use of this computer system by any person, whether authorized or unauthorized, constitutes consent to these terms. There is no right of privacy in this system. "

For Windows NT/2000:

Set OS version equal or greater to Windows NT/2000

Add the following to the system registry:

[HKEY_LOCAL_MACHINE \SOFTWARE \Microsoft \Windows NT\CurrentVersion \Winlogon]

"LegalNoticeCaption"=" Warning Notice! "

"LegalNoticeText"=" This is a GIAC Healthcare computer system, which may be accessed and used only for authorized GI AC Healthcare Systems' business by authorized personnel. All information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Access or u se of this computer system by any person, whether authorized or unauthorized, constitutes consent to these terms. There is no right of privacy in this system. "

Implementation by Semi -manual Means: [v]

A manual method can b e utilized by making an importable registry file – one for Windows 9X and one for Windows 2000/NT, due to differences in the registries. In addition, two more registry files should be considered as to restore the settings back to normal in case of trouble.

Using the Windows utility notepad, create two files, one for each core Windows operating system, which will contain the registry key values to be assigned. Name the first file *W9X_banner.reg*. A second file should be created named *W2K_NT_banner.reg*. The .reg suffix indicates that the file is a Regedit registry data file.

Create the registry file - the below can be cut and pasted into the correct registry file:

For Windows 9x:

W9X_banner.reg

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current
Version\Winlogon]

"LegalNoticeCaption"= "Warning Notice!"

"LegalNoticeText"="This is a GIAC Healthcare computer system,
which may be accessed and used only for authorized GIAC
Healthcare Systems' business by authorized personnel. All
information on this computer system may be intercepted, recorded,
read, copied, and disclosed by and to authorized personnel for official
purposes, including criminal investigations. Access or use of this
computer system by any person, whether authorized or unauthorized,
constitutes consent to these terms. There is no right of privacy in this
system."

"@"=
```

For Windows NT/2000:

Note: The installer must be logged in as an administrative user (one in the Administrators group) or have local administers privileges.

W2K_NT_banner.reg

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon]

"LegalNoticeCaption"=" Warning Notice!"

"LegalNoticeText"="This is a GIAC Healthcare computer system,
which may be accessed and used only for authorized GIAC
Healthcare Systems' business by authorized personnel. All
information on this computer system may be intercepted, recorded,
read, copied, and disclosed by and to authorized personnel for official
purposes, including criminal investigations. Access or use of this
computer system by any person, whether authorized or unauthorized,
constitutes consent to these terms. There is no right of privacy in this
system."

"@"=
```

Notes:

Ensure that no end-of-line characters appear within the text lines. The values assigned must be continuous strings, without embedded end-of-line characters. To check for undesired end-of-line characters in the Notepad program, deselect Word Wrap in the Edit menu, and see if any of the assigned values span multiple lines. If so, remove the end-of-line character between the split lines.

Ensure that the entered data is correct and save the file.

To execute Regedit.exe with the appropriate .reg file to have the new values entered into the registry, double-click on the appropriate .reg file that is relevant to the operating system of the personal computer or right click on the appropriate .reg file and click on "merge".

Select OK to continue. A message will appear, indicating that the values in the file have been entered into the registry.

To verify that the logon banner has been correctly entered, log out and then log in again. You should be presented with the logon banner that requires you to select OK before proceeding to the logon prompt.

As an aid to troubleshooting and as a best practice, a reversal of the registry can be accomplished via merging in the following registry files.

For Windows 9x:

W9X_banner_restore.reg

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Winlogon]

"LegalNoticeCaption"=""

"LegalNoticeText"=""

"@"=
```

For Windows NT/2000:

Note: The installer must be logged in as an administrative user (one in the Administrators group) or have local administers privileges.

W2K_NT_banner_restore.reg

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]

"LegalNoticeCaption"=""
```

```
"LegalNoticeText"=""

"@"=
```

The Paper’s Definitions

Audit Trail: An audit control or a system of record keeping. The audit trail tracks activities sufficiently to enable a reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction, from its inception to output of final results. The audit trail must be designed to meet the legal record keeping requirements of such transaction activities.

ACL: Access Control List, a set of data that informs a computer's operating system which permissions, or access rights, that each user or group has to a specific system object, such as a directory or file. Each object has a unique security attribute that identifies which users have access to it, and the ACL is a list of each object and user access privileges such as read, write or execute. [vi]

CHAP: Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCI Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.

Confidential: “Confidential Information,” for purposes of this policy, is defined as information that is valuable and private and is protected by law and/or Bon Secours Health System policies. Confidential information includes, but is not limited to: (1) patient identifiable health, demographic and/or payment-related information or such information that can be used to identify a patient; (2) employee information that is private such as salaries, employment records, and disciplinary actions; (3) Bon Secours Health System business information that is not available from public sources such as Bon Secours Health System annual reports, American Hospital Association and other health care industry publications, and federal/state available data; and, (4) third party proprietary information such as computer programs, source code, and technology specifications.

HIPAA: The Health Insurance Portability & Accountability Act of 1996 (August 21), Public Law 104-191, which amends the Internal Revenue Service Code of 1986. Also known as the Kennedy-Kassebaum Act.

HIS: Abbreviation for “Hospital Information System”. This term encompasses one large application with modules or a multitude of smaller applications that support each modality of the healthcare process.

ISDN: Abbreviation of integrated services digital network, an international communications standard for sending voice, video, and data over digital telephone lines or normal telephone wires. ISDN supports data transfer rates of 64 Kbps (64,000 bits per second). Most ISDN lines offered by telephone companies give you two lines at once, called B channels. You can use one line for voice and the other for data, or you can use both lines for data to give you data rates of 128 Kbps, three times the data rate provided by today's fastest modems. [vii]

NOC: The Network Operations Center, the physical space from which a typically large telecommunications network is managed, monitored and supervised. The NOC coordinates network troubles, provides problem management and router configuration services, manages network changes, allocates and manages domain names and IP addresses, monitors routers, switches, hubs and UPS systems that keep the network operating smoothly, manages the distribution and updating of software and coordinates with affiliated networks. NOCs also provide network accessibility to users connecting to the network from outside of the physical office space or campus. [viii]

PHI: Protected Health Information (individually identifiable health information such as name, medical record number, diagnosis, etc.)

PRI: Primary Rate Interface, a type of ISDN service designed for larger organizations. PRI includes 23 B -channels (30 in Europe) and one D-Channel. In contrast, BRI (Basic Rate Interface), which is designed for individuals and small businesses, contains just two B - channels and one D -channel. [ix]

Script Kiddie : A person, normally someone who is not technologically sophisticated, who randomly seeks out a specific weakness over the Internet in order to gain root access to a system without really understanding what it is s/he is exploiting because the weakness was discovered by someone else. A script kiddie is not looking to target specific information or a specific company but rather uses knowledge of a vulnerability to scan the entire Internet for a victim that possesses that vulnerability. [x]

Sniffing: The use of a program and/or device that monitors data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere. This makes them a favorite weapon in the hacker's arsenal. [xi]

Works Cited

[i] Health Insurance Portability and Accountability Act of 1996 – Title II – Preventing HealthCare Fraud and Abuse; Administrative Simplification; Medical Liability Reform, Part C – Administrative Simplification. Online. Internet. 14 Sep. 2002. http://aspe.hhs.gov/admnsimp/pl104191.htm#1177

[ii] Health Insurance Portability and Accountability Act of 1996 – Title II – Preventing HealthCare Fraud and Abuse; Administrative Simplification; Medical Liability Reform, Part C – Administrative Simplification. Online. Internet. 14 Sep. 2002. http://aspe.hhs.gov/admnsimp/pl104191.htm#1176

[iii] http://www.sans.org/newlook/resources/policies/Remote_Access_Po licy.doc Online. Internet. 14 Sep. 2002.

[iv] http://www.novell.com/coolsolutions/gov/features/trenches/tr_workstation_warnings_gov.html Online. Internet. 25 Sep. 2002.

[v] http://www.cert.org/security -improvement/implementations/i034.01.html Online. Internet. 17 Sep. 2002.

[vi] http://www.webopedia.com/TERM/A/ACL.html Online. Internet. 17 Sep. 2002.

[vii] http://www.webopedia.com/TERM/I/ISDN.html Online. Internet. 15 Sep. 2002.

[viii] http://www.webopedia.com/TERM/N/NOC.html Online. Internet. 15 Sep. 2002.

[ix] http://www.webopedia.com/TERM/P/PRI.html Online. Internet. 17 Sep. 2002.

[x] http://www.webopedia.com/TERM/S/script_kiddie.html Online. Internet. 15 Sep. 2002.

[xi] http://www.webopedia.com/TERM/s/sniffer.html Online. Internet. 23 Sep. 2002.