

Establishing a Secure, HIPAA-Compliant Network Perimeter

DISCUSSION POINTS

- ☞ EXECUTIVE SUMMARY
- ☞ DEFINING THE RISK OF PERIMETER SECURITY BREACHES
- ☞ PERIMETER SECURITY IN THE HEALTHCARE INDUSTRY
- ☞ WHAT DO HACKERS LOOK FOR?
- ☞ HIPAA AND PERIMETER SECURITY
 - Administrative Procedures
 - Technical Security Mechanisms
- ☞ STRATEGIES TO CREATE A SECURE, HIPAA-COMPLIANT PERIMETER
 - Step #1—Define the Perimeter
 - Step #2—Test for Security Vulnerabilities
 - Step #3—Reconfigure Existing Technologies and Deploy New Technologies
 - Step #4—Revise Ineffective Policies and Procedures
 - Step #5—Manage and Monitor Perimeter Security
- ☞ ABOUT RIPTECH
- ☞ SOURCES

EXECUTIVE SUMMARY

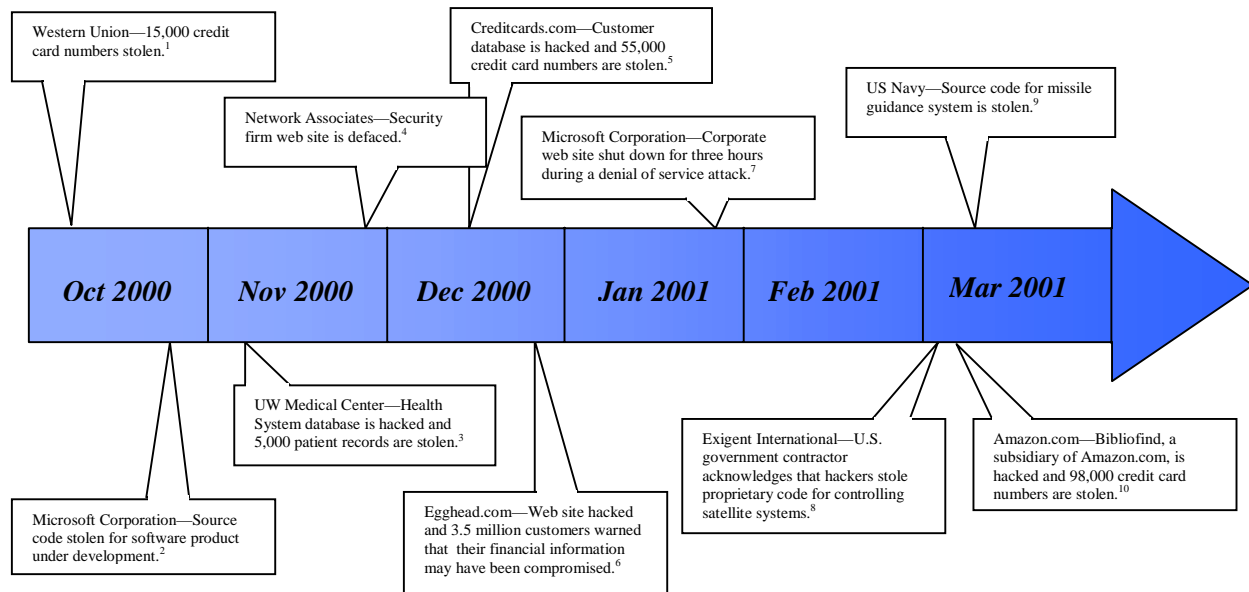
Given the dramatic rise in external security threats, coupled with the rising cost of network intrusions, organizations across industries are more pressured than ever to define and protect their network perimeter. This pressure is particularly intense at healthcare organizations, such as health insurance companies and hospitals, due to the particularly sensitive nature of medical information. Under increasing pressure from consumers and the federal government to improve their security postures, many healthcare IT executives are scrambling to identify and eliminate security holes that render their network vulnerable to external security threats. However, faced with continuing cost pressures and IT staffing shortages, healthcare organizations are unfortunately handicapped in their ability to recruit qualified staff to establish and maintain an effective information security posture.

In order to address these concerns, this white paper provides an overview of the different types of perimeter vulnerabilities to which healthcare organizations are commonly exposed and defines the risk that these vulnerabilities pose to an organization. The paper then goes on to explain how healthcare organizations should go about eliminating these security vulnerabilities, thereby reducing their business risk and demonstrating due diligence in complying with a key set of HIPAA Security requirements. After reading this paper, healthcare IT executives will understand at a high level what actions that they must take in order to establish and maintain a secure, HIPAA-compliant network perimeter.

DEFINING THE RISK OF PERIMETER SECURITY BREACHES

Businesses today face major information security risks as technologies, such as the Internet, render proprietary networks more exposed than ever to external threats. Virtually every day, a well-known company announces that a hacker has infiltrated its network and, in many cases, has caused significant financial damage. The graphic below highlights just a small sampling of network intrusions announced at major corporations throughout the past six months.

TIMELINE OF HIGH PROFILE NETWORK INTRUSIONS



Recent survey data, collected through a joint effort by the FBI and Computer Security Institute (CSI), confirms what many organizations have experienced first-hand—corporate networks throughout the world are more prone than ever to intrusions originating from outside of the network perimeter. In fact, contrary to popular belief, the majority of organizations (approximately 70%) report that Internet connections are the most frequent source of security breaches, as opposed to breaches originating from inside the network.¹¹

Unfortunately, despite the growing awareness of this risk, many organizations continue to maintain ineffective security postures on the network perimeter. After reviewing the results of the FBI/CSI survey, Patrice Rapalus, CSI Director, supports this sentiment:

“The survey results over the years offer compelling evidence that neither technologies nor policies alone really offer an effective defense for your organization. Intrusions take place despite the presence of firewalls....Organizations that want to survive in the coming years need to develop a comprehensive approach to information security, embracing both the human and technical dimensions.”¹²

PERIMETER SECURITY IN THE HEALTHCARE INDUSTRY

Drawing from the experiences of the Riptech Security Professional Services (SPS) engineers, it is clear that inadequate security practices on the network perimeter are significantly more acute in the healthcare industry, particularly in the healthcare provider market. Hampered by severe cost constraints, IT staffing shortages, and large, fragmented information networks, healthcare organizations often lack the resources, expertise, and empowerment to establish and maintain a secure network perimeter.

Fortunately, as these organizations prepare for compliance with the pending HIPAA Security Rule, many are beginning to recognize the inherent business risks of maintaining an ineffective security posture on the network perimeter. Due to the fact that risk is difficult to quantify with information security issues, the following table highlights some of the major types of risks that healthcare organizations face in the event of an unauthorized network intrusion.

RISK	EXPLANATION
Civil Lawsuits	Many legal experts believe that even before the HIPAA Security Rule goes into effect, healthcare organizations will be sued in state courts under tort law and various contract theories if patient information is compromised and released. While precedence for lawsuits remains uncertain, this represents a significant risk that healthcare organizations must address today.
Federal Fines	The HIPAA Security Rule establishes monetary (and potentially criminal penalties) for healthcare organizations that fail to comply with the requirements. In the event of a violation, organizations are subject to a \$250 fine per incident and up to \$250,000 per year per violation type. ¹³
Compromised Patient Care	Once inside the network perimeter, there is the potential for hackers to actually impact the quality of patient care. Databases housing patient records, lab results, etc., could potentially be altered and have a devastating impact on patient care.
Tarnished Corporate Reputation	Healthcare organizations typically store a wealth of confidential corporate and patient care data that, if released, could have a devastating impact on public perception. For instance, by law, hospitals must record each instance of a medical error that occurs at the facility. If this information were released to the public, the effects could be unrecoverable.

WHAT DO HACKER'S LOOK FOR?

In order to understand why organizations frequently suffer network intrusions (and how these can be avoided), it is important to first gain a high level understanding of the different types of vulnerabilities that hackers seek when casing a network. While days can be spent detailing a virtual endless list of specific vulnerabilities, it is more helpful to healthcare IT executives to obtain a high level overview of the different categories of vulnerabilities. Once organizations have a firm understanding of the various categories, steps can be taken to identify and eliminate them. The table below lists the categories of vulnerabilities that hackers typically search for:

VULNERABILITY	EXPLANATION
<p>Inadequate Border Protection</p>	<p>Perhaps the easiest way to penetrate a network is to identify an Internet Gateway with inadequate border protection. In simple terms, this situation occurs when an organization fails to install a firewall to separate the public Internet from a private network. The simple rule of thumb here is that every Gateway to the Internet MUST have a well-configured firewall between the private network and the public Internet. Those that do not will inevitably suffer an attack from the outside.</p> <p><i>Example: University of Washington Medical Center</i>—The absence of a firewall, coupled with weak user name and password policies, allows a hacker to enter a corporate database and download 5,000 patient medical records.¹⁴</p>
<p>Remote Access Systems (RAS) with Weak Access Controls</p>	<p>If hackers are unable to gain access to a network through an Internet Gateway, an easy way to bypass the Gateway is to exploit remote access systems (RAS) with weak access controls. Remote access vulnerabilities (such as dial-in servers) are a frequent point of access for hackers that are unable to compromise access controls protecting the Gateway, such as a well-configured firewall. By dialing directly into a server, hackers can access the network without passing through the firewall.</p> <p><i>Example: Several attacks on major corporate networks by Kevin Mitnick</i> were enabled by exploiting dial-up vulnerabilities.</p>
<p>Application Servers with Well-Known Exploits</p>	<p>Many application servers, such as web servers, rely on well-known scripts that suffer from equally well-known vulnerabilities. Failure to patch or replace these scripts renders these servers vulnerable to attack.</p> <p><i>Example: Egghead.com</i>—Web server vulnerabilities enable a hacker to access a database containing 3.5 million customer credit card numbers. Web defacements and credit card theft, such as this example, are often made possible by web server vulnerabilities.¹⁵</p>
<p>Misconfigured Systems and Systems with Default Configurations</p>	<p>Many operating systems and applications (such as a firewall application) are misconfigured or installed using default configurations. While default configurations expedite installation, such practices often introduce a host of vulnerabilities that hackers can easily exploit. Default installations include vulnerabilities such as the availability of high-risk services and default user accounts with known passwords. Once a hacker identifies a target, often the next step is to locate a system with default configurations or common misconfigurations.</p> <p><i>Example: Microsoft Corporation</i>—In October 2000, a hacker identified a server that had an administrator account with a blank password. By gaining access to this server, the hacker was able to view the source code for a software program in development. After investigating the incident, Microsoft discovered that IT staff failed to change the blank password when installing the server.¹⁶</p>

HIPAA AND PERIMETER SECURITY

The HIPAA Security Rule was intended to serve as a “best practices” guideline that healthcare organizations must use to eliminate the types of vulnerabilities described on the previous page. With regard to the network perimeter, the HIPAA requirements can be broken down into two types. The first set of requirements, referred to in HIPAA as “Administrative Procedures,” outline the types of managerial policies and procedures that healthcare organizations must implement in order to maintain a sound security posture. The second set of requirements, referred to in HIPAA as “Technical Security Mechanisms,” outline the actual technical security features that organizations must have in place to ensure network security when the organization uses communications (e.g., Internet connectivity) and/or network controls (e.g., firewalls). Each set of requirements is explained below and on the following page in greater detail.

❖ *Administrative Procedures*

Although most of the “Administrative Procedures” outlined in the HIPAA Security Rule are non-technical in nature, there are three implementation features that directly apply to an organization’s security posture on the network perimeter. Each of these requirements is outlined and explained in the table below.

REQUIREMENT*	IMPLEMENTATION FEATURE	DESCRIPTION
Security Configuration Management	Hardware/Software Installation, Maintenance, Review, and Testing for Security Features	Requires organizations to establish formal documented procedures for connecting and loading new equipment and programs, periodically reviewing the maintenance occurring on that equipment and programs, and periodic security testing of the security attributes of that hardware/software. With regard to the network perimeter, this implementation feature requires organizations to establish and apply these procedures to the installation and maintenance of application servers (such as web servers) and other perimeter systems.
	Security Testing	Requires organizations to establish a process to ensure that the security features of a system are implemented as designed and that they are adequate for a proposed applications environment. This process includes hands-on functional testing, penetration testing, and verification. With regard to the network perimeter, this implementation feature requires organizations to test perimeter systems and security technologies regularly to ensure that they perform as intended.
Internal Audit	None	Requires organizations to conduct a periodic review of the records of system activity (such as logins, file accesses, and security incidents). With regard to the network perimeter, this provision requires healthcare organizations to review audit data, such as firewall logs and intrusion detection alerts, to identify instances of suspicious network activity.
* Each of the requirements outlined in this table apply to an organization’s internal network and network perimeter. Since this white paper is only focused on perimeter security, these requirements are only explained in this context.		

Source: “Security and Electronic Signature; Proposed Rule.” *Federal Register*. (August 12, 1999): pp. 43266.

In essence, the “Administrative Procedures” require healthcare organizations to establish a documented set of policies and procedures to eliminate the vulnerabilities described in the previous section. When applied to the perimeter, the intention is to force organizations to continually examine network architecture, system and application configuration, security product selection, and security audit data to ensure that the network perimeter is protected from external threats.

❖ *Technical Security Mechanisms*

The “Technical Security Mechanisms” section of the HIPAA Security Rule outlines a number of technical features that a healthcare organization must have in place when using communications and/or network controls. With regard to perimeter security, there are four implementation features outlined in the “Technical Security Mechanisms” section that healthcare organizations must have in place to adequately protect the network perimeter when using open networks, such as the Internet. Each implementation feature is outlined and briefly described below.

REQUIREMENT	IMPLEMENTATION FEATURE	DESCRIPTION
Communications/ Network Controls Internal Audit	Entity Authentication	Requires organizations to have a communications or network mechanism to irrefutably identify authorized users, programs, and processes and to deny access to unauthorized users, programs and processes. This implementation feature requires organizations to use technology, such as firewalls, to govern which users, programs, and processes are allowed to access the private network through the Internet.
	Alarm	Requires organizations to use a device that can sense an abnormal condition with the system and provide, either locally or remotely, a signal indicating the presence of the abnormality. This implementation feature seems to require intrusion detection technology, which alerts network administrators to suspicious network activity.
	Event Reporting	Requires organizations to use technology that indicates the presence of operational irregularities in physical elements of a network or a response to the occurrence of a significant task. This feature seems to require the use of intrusion detection technologies and/or security devices that are capable of reporting security device failures.
	Audit Trail	Requires organizations to use technologies that collect data that can be used to facilitate a security audit. This implementation feature requires healthcare organizations to collect and store data, such as firewall logs, to be used during periodic security audits.

Source: “Security and Electronic Signature; Proposed Rule.” *Federal Register*. (August 12, 1999): pp. 43268.

In essence, the implementation features described above require healthcare organizations to use technology solutions that provide reasonable safeguards to protect against unauthorized access to proprietary networks through open networks, such as the Internet. These implementation features also outline the types of data that security devices, such as firewalls and intrusion detection systems, must generate in order to equip security managers with the information that they need to monitor security and conduct a security audit. When applied to the network perimeter, the intention of this requirement is to force organizations to continually review the capabilities and performance of security technologies that protect the network perimeter.

STRATEGIES TO CREATE A SECURE, HIPAA COMPLIANT PERIMETER

Given the substantial financial risk of network intrusions, coupled with strict HIPAA Security requirements, healthcare organizations must act now to ensure that appropriate technologies and management practices are adopted and maintained to protect against current and future threats. This section outlines a logical four-step process that healthcare organizations should follow to establish and continuously manage and monitor an effective security posture on the network perimeter. Riptech offers several services to support healthcare organizations throughout each step.

❖ *STEP #1—Define the Perimeter & Test for Vulnerabilities*

The obvious first step in securing the network perimeter is to define the bounds of the network and map each potential remote access point. While this seems rather straightforward in theory, in reality many healthcare organizations do not have an accurate map of their network perimeter and are therefore unable to easily identify all of the vulnerabilities that may be leveraged by an external attacker. When defining the network perimeter, healthcare organizations should look for access points, such as the following.

NETWORK CONNECTIVITY	REMOTE ACCESS
<ul style="list-style-type: none"> • Internet Gateways • Wide Area Network (WAN) connections • Private lines with business partners 	<ul style="list-style-type: none"> • Virtual Private Networks (VPNs) • Remote Access Systems (e.g., Citrix servers) • Rogue modems • Known dial-in servers

Once the network perimeter is completely mapped, a healthcare organization is ready to examine each remote access point to isolate security vulnerabilities. During this stage of the assessment, healthcare organizations should search for the four types of technical vulnerabilities outlined earlier in this white paper. Examples of these vulnerabilities are briefly summarized below.

VULNERABILITY	EXAMPLE
Inadequate Border Protection	<ul style="list-style-type: none"> • Failure to install a firewall to protect an Internet Gateway • Failure to install network-based intrusion detection system to monitor traffic on critical network segment
RAS Vulnerabilities	<ul style="list-style-type: none"> • Unauthorized deployment of PC Anywhere on a server • Poor password selection on Citrix dial-in server
Application Server Vulnerabilities	<ul style="list-style-type: none"> • Failure to patch a web server, which renders the server prone to attack using well-known exploits • Failure to patch firewall, which renders Internet Gateway prone to a newly discovered exploit
Misconfiguration Vulnerabilities and Default Configurations	<ul style="list-style-type: none"> • Misconfigured router that renders organization more susceptible to denial of service attacks • Open rule sets on a firewall that permit the use of Trojan software • OS configuration on a perimeter system that allows hackers to exploit default user names and passwords
Riptech Service: Perimeter Assessment	

❖ **STEP #2—Reconfigure Existing Technologies and Deploy New Technologies**

Once healthcare organizations have a firm understanding of the technical vulnerabilities that exist on the network perimeter, IT staff can reconfigure existing technologies and/or purchase new security technologies to eliminate these vulnerabilities. Several options that healthcare organizations should consider are described in the following table.

RECONFIGURATION CONSIDERATIONS	
OS Hardening	Operating systems of many perimeter systems will likely require reconfiguration (commonly called hardening) to eliminate default configurations and unnecessary services that render the system more vulnerable to attack.
Application Patching	Many application servers (e.g., web, email, ftp, etc.) will require patching to eliminate common vulnerabilities.
Application Reconfiguration	Many security applications, such as firewalls, must be reconfigured to protect against emerging security vulnerabilities.
Password Changes	Many remote access passwords, such as (default passwords on PC Anywhere) must be changed in order to protect against brute force password attacks on vulnerable dial-in servers.
Elimination of Rogue Modems	Modems connected to servers should be disconnected unless these are absolutely required by the healthcare organization. This minimizes the likelihood of successful dial-in attacks.
Riptech Service: Customized Security Engineering	

TECHNOLOGY CONSIDERATIONS	
Firewalls	Organizations must deploy firewalls to protect critical network connection points, such as Internet Gateways and WAN connection points.
VPNs	Organizations should consider using technology, such as VPNs, when users are provided with access to internal network resources via the Internet.
Intrusion Detection	Organizations must consider the deployment of intrusion detection technology to generate alerts in the event of suspicious network activity (e.g., port scanning) on the network perimeter.
Strong Authentication	Organizations should consider the use of strong authentication technology (such as token systems) to protect remote access systems.
Riptech Service: Security Product Implementations	

❖ **STEP #3—Revise Ineffective Policies and Procedures**

In addition to establishing a solid baseline security posture on the network perimeter, healthcare organizations must review and revise policies and procedures to ensure that the same level of security is maintained in the future. In order to provide this assurance, healthcare organizations should review and revise policies and procedures, such as:

POLICY	DESCRIPTION
Passwords	Organizations should establish a policy governing password selection and maintenance for dial-in systems, operating systems on perimeter devices, VPNs, etc. A strict password policy ensures that systems cannot be compromised with password guessing tools.
Remote Dial-in	Organizations should establish a policy regarding the deployment of remote dial-in services, such as PC Anywhere. The policy should outline protocols for introducing and managing new dial-up points on the network.
Internal Audit	Organizations should establish clear policies and procedures for regularly auditing security data, such as firewall logs. Regular audits ensure that intrusion attempts are identified and deflected before damage occurs.
Configuration Guidelines	Organizations should establish clear guidelines for the configuration of perimeter systems and applications, such as firewalls, web servers, dial-in servers, etc. Configuration guidelines ensure that common vulnerabilities do not occur when systems are reconfigured or new systems are installed.
Riptech Service: Security Policy Development	

❖ **STEP #4—Manage and Monitor Perimeter Security**

Upon establishing a baseline technical and administrative security posture on the network perimeter, healthcare organizations must continually manage and monitor security to defend against network intrusion attempts and eliminate new vulnerabilities as they emerge. In addition to adhering strictly to the policies and procedures outlined in **Step #3**, healthcare organizations should consider the following types of services.

SERVICE	DESCRIPTION
Managed Security Services	Organizations should consider outsourcing the 24x7 management and monitoring of network security devices, such as firewalls and intrusion detection systems. Managed security services, such as those offered by Riptech, provide organizations with two valuable benefits, which are key to maintaining a secure, HIPAA-compliant network perimeter. The specific benefits of Riptech's services are summarized below. <ul style="list-style-type: none"> • <i>24x7 Security Monitoring & Analysis</i>—Riptech analyzes security data in real-time to provide organizations with immediate notification and response guidance when suspicious network activity occurs. • <i>Security Configuration Management</i>—Riptech provides organizations with best-practices configuration and product maintenance to ensure optimal performance of perimeter security devices.
Perimeter Security Assessments	Organizations should outsource periodic perimeter assessments to ensure that vulnerabilities, such as those described in Step #1 , do not re-occur.
Riptech Services: <ul style="list-style-type: none"> • Managed Security Services • Perimeter Assessments 	

ABOUT RIPTECH

Riptech, Inc., the only provider of real-time managed security services, protects clients through advanced outsourced security monitoring and professional services. Riptech's unique CaltarianSM technology platform provides real-time information protection through around-the-clock monitoring, analysis, and response. Riptech offers the only technology capable of processing large volumes of network security data to separate security threats from false positives in real-time, with nearly limitless scalability. Additionally, Riptech's Security Professional Services group provides security policy development, assessment and auditing, penetration testing, incident forensics, and response. Riptech security specialists have secured hundreds of organizations including Fortune 500 companies and federal agencies. Founded in 1998 by former Department of Defense security professionals and market experts, Riptech is headquartered in Alexandria, Virginia with offices in San Jose, California, and Philadelphia, Pennsylvania.

SOURCES

- ¹ "Hackers Break Into Site, Western Union Reports." *New York Times*. (September 11, 2000).
- ² "Microsoft Infiltrated By Hackers." *Washington Post*. (October 28, 2000).
- ³ Songini, M. "Hospital Confirms Hacker Stole 5,000 Patient Files." *Computerworld*. (December 18, 2000).
- ⁴ Delio, M. "Security Firm's Site Defaced." *Wired News*. (November 30, 2000).
- ⁵ Atanasov, M. "The Truth about Internet Fraud." *ZDNet*. (April 1, 2001).
- ⁶ Harris, R. "Online Retailer Egghead.com Hacked." *AP Online*. (December 22, 2000).
- ⁷ Delio, M. "A Bad Day for Microsoft." *Wired News*. (January 24, 2001).
- ⁸ Lemos, R. "Contractor: Satellite Code Hackers Broke In." *ZDNet*. (March 2, 2001).
- ⁹ Soltis, A. "Hackers Heist Navy's Missile Codes." *New York Post*. (March 3, 2001).
- ¹⁰ Evers, J. "Amazon Unit Loses Credit Card Data to Hackers." *InfoWorld Daily News*. (March 6, 2001).
- ¹¹ "Financial Losses Due to Internet Intrusions, Trade Secret Theft and Other Cyber Crimes Soar." *Computer Security Institute Press Release*. (March 12, 2001).
- ¹² Ibid.
- ¹³ "Security and Electronic Signature Standards; Proposed Rule." *Federal Register*. (August 12, 1998).
- ¹⁴ Songini, M. "Hospital Confirms Hacker Stole 5,000 Patient Files." *Computerworld*. (December 18, 2000).
- ¹⁵ Harris, R. "Online Retailer Egghead.com Hacked." *AP Online*. (December 22, 2000).
- ¹⁶ Dudley, B. "Microsoft Executive Tells How Hacker Got In." *Seattle Times*. (February 23, 2001).