Healthcare and Public Health Cybersecurity Primer: Cybersecurity 101

Healthcare and Public Health Sector

Cybersecurity Working Group

The Cybersecurity Working Group give special thanks to all of the Healthcare and Public Health Sector partners from the private sector as well as State, local, tribal, territorial, and Federal agencies who aided in the development of this document. Your continued dedication to the protection and resilience of healthcare and public health critical infrastructure is greatly appreciated.

Foreword

The document *Healthcare and Public Health Cybersecurity Primer: Cybersecurity 101* was developed by the Healthcare and Public Health (HPH) Sector Cybersecurity Working Group (CSWG). The Cybersecurity Working Group (CSWG) directs the HPH sector's cybersecurity analysis, education, and awareness efforts, to include coordinating with the Risk Management Working Group to provide cybersecurity expertise for the sector's risk management objectives.

The CSWG is comprised of public and private sector entities and organizations that coordinate under the Critical Infrastructure Partnership Advisory Council (CIPAC) framework. The CIPAC framework and related guidelines were established based on the critical need for effective information sharing between then private sector and Federal, state, local, tribal and territorial entities throughout the United States. CIPAC allows real time, continuous communications and open dialogue among a wide variety of constituents. According to the CIPAC charter:

> The Secretary, Department of Homeland Security, has exercised statutory authority to exempt CIPAC meetings from the requirements of the Federal Advisory Committee Act. That exemption was expressly provided to establish a known and trusted framework that would:
>
> - Facilitate the flow of advice and information concerning critical infrastructure protection;
> - Foster effective information sharing;
> - Mitigate the risk of compromising vulnerabilities; or that would promote necessary communications during emergencies.

The Healthcare and Public Health Cybersecurity Primer aims to leverage this framework to present introductory information on cybersecurity to healthcare and public health professionals.

Table of Contents

1.0 Introduction

The Department of Homeland Security and the Department of Health and Human Services have identified that the Healthcare and Public Health (HPH) sector remains at risk from opportunistic and targeted cyber incidents that continue to grow in number and sophistication. In March 2009, the Director of National Intelligence testified before Congress that "the growing connectivity between information systems, the Internet, and other infrastructures creates opportunities for attackers to disrupt telecommunications, electrical power, energy pipelines, refineries, financial networks, and other critical infrastructure."[1] The White House *Cyberspace Policy Review* further reinforced the risks to critical infrastructure, citing Central Intelligence Agency reports of malicious activities against information technology (IT) systems that caused the disruption of electrical power infrastructure in multiple regions overseas, and the growing risk "as digital and network technologies are being integrated across large systems."[2] These cyber threats have the potential to cripple owners and operators and to disrupt critical services.

The Healthcare and Public Health (HPH) sector is a large and diverse sector that provides a vast array of goods and services that are essential to the health, safety and well-being of the Nation. Critical functions of the sector include, but are not limited to:

- Acute care hospitals and ambulatory healthcare including the doctors, nurses, occupational health practitioners that support those facilities;
- Health plans and payers, who provide payment to caregivers for goods and services related to healthcare;
- Mass Casualty and Mortuary care;
- A large system of private sector enterprises that manufacture, distribute, and sell, drugs, biologics and medical devices; and
- Population-based care and surveillance provided by health agencies at the Federal, State, and local levels.

In each of the above-listed critical functional areas, the HPH sector has become more reliant on technology to support and improve the provision of care, disease prevention, and emergency response. However, since sector stakeholders are focused on providing quality care and saving lives, the cyber dimension of the sector can sometimes be viewed as secondary, or not part of the professional knowledge base. With the proliferation of health information technology and cyber systems within the critical functions of the HPH sector, there is a compelling need to address and manage the risks associated with cyber threats to HPH.

Understanding the evolving role of cybersecurity in healthcare and public health is a crucial first step to managing cyber risks to the HPH sector. The *Healthcare and Public Health Cybersecurity Primer* is a tool intended for use by sector members, owners and operators, as well as Federal, State and local partners who may not be cyber experts, but wish to improve the sector's level of understanding of

1 Director of National Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Armed Services Committee, Statement for the Record*, March 10, 2009.

2 White House, *Cyberspace Policy Review*, May 2009, p. 2.

cybersecurity.[3] The scope of this document contains concepts and common practices of security as they pertain to the cyber component of healthcare and public health.[4] This document will:

- Provide a basic definition of cybersecurity;
- Discuss qualities of a secure cyber environment;
- Present a high level examination of cyber threats and consequences and vulnerabilities; and
- Discuss preventative measures and recommended risk management activities.

The document will conclude with a guide to further resources on cyber issues and will also provide a glossary of common terms.

[3] This document also supports the national policies established by the Homeland Security Presidential Directive-7, which calls for coordination between public and private entities to enhance the protection and resilience of the Nation's critical infrastructure.

[4] It is important to note here that this document will not address healthcare privacy issues, which present cyber liability concerns outside the scope of this document.

2.0 Qualities of a Secure Cyber Environment

In its most basic form, security ensures the integrity of data and its availability to the appropriate and/or designated persons. The term *cybersecurity* refers to the protection of cyberspace[5] and related technologies, from records and electronic data to the physical structures of security systems. Cybersecurity, as it applies to the Healthcare and Public Health Sector, encompasses the defensive measures and activities that prevent exploitation or misuse of the cyber infrastructure within the sector. This includes – but is not limited to – medical devices, laboratory systems and networks, hospital and treatment center information systems, patient databases, hardware components, and software.

Applied correctly, cybersecurity mechanisms and techniques may help prevent attacks on systems and networks. An attack can be defined as any action that hinders normal functionality or normal system operations or allows an unwanted individual or group access to a system or network. Cybersecurity can help to manage or mitigate risks resulting from in from nefarious actors, malware, and broad information sharing. It can streamline auditing, reporting, configuration management and system patching. As much as the cyber dimension connects multiple types of infrastructure, it is a constantly evolving network with ever-changing threats and vulnerabilities to discover evaluate and manage. Thus, securing cyber space is quite a challenge. Threats are becoming even more sophisticated while security technology strives to keep the same pace. Much of this technology requires specialized training and continuous monitoring, as well as high costs.

Organizations struggle with prioritizing and implementing security requirements. Since technology and security do not advance in sync with one another, the threat environment sometimes evolves at a faster rate than the security measures. Basic security and protective measures should always be employed, but it should be well understood that they are not necessarily sufficient to protect against any attacks. Systems and networks in the sector that are most at risk are those without even the basic or minimum protections. As the complexity of attacks continues to evolve and sector infrastructure is increasingly reliant on networks, owners and operators of systems and networks must be prepared to quickly adjust security measures. Security measures must be dynamic, up-to-date, and employ commonly accepted practices at all times.

In the world of cybersecurity, any system or network is only as good as the weakest link in that particular system or network. Listed below are commonly recognized practices and that serve to enhance network securities and can be widely applied to the many facets of the HPH sector. This list is not intended to be all-inclusive; however, should be considered the minimum level of protection, because without them a system or network would be completely exposed.

Identification and Authentication is the ability to validate an individual, device, or a process prior to accessing or carrying out an activity on a given system or network. This provides owners and operators with a mechanism to identify the actor(s) involved in a transaction and create a framework for auditing

[5] National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD23) defines cyberspace as "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries." Common usage of the term also refers to the virtual environment of information and interactions between people.

users' actions. Security controls can be employed at different levels depending on the authentication need. A common example is a user ID and password.

Security Patch Management is the process of updating software to reduce the risk of compromise to applications, systems, and computers as a result of system flaws, thus it is more of a reactive response to a discovered vulnerability. Patching is a proactive risk management approach to system security. This action protects systems from compromises from malfunctioning software and other programs. A patch, which is applied as an update to a system or software package, is code that is deployed into software to fix a bug or vulnerability. However, complicated medical devices designed to carry out complex health-related functions could be compromised as a result of improper patch application. Thus, experienced IT professionals should always be consulted in the application of security patches.

Firewalls are the first line of defense against unwanted network intrusions. They enable a layered security approach and, to the extent possible, provide assurance that a system is protected from malicious actors. There are several different types of firewalls; the necessity for level of protection will depend on the complexity and sensitivity of the system it protects. Firewalls manage the traffic entering and leaving a network by applying any of four different mechanisms to restrict traffic—packet filtering, circuit-level gateway, proxy server and application gateway. The packet filtering allows the firewall to perform packet inspections to ensure the data entering your infrastructure is safe. Organizations can develop business rules to limit what is allowed in or out. Firewalls are best utilized either at the perimeter of the network or between the network infrastructure and the Internet.

Encryption ensures that computers are not accesses by anyone other than a specific authorized user and devices adequately maintain the integrity and reliability of electronic information. There are two types of encryption:

- *Storage*—this type of encryption can be applied to mobile devices, electronic media, laptops, desktop, servers where sensitive data is stored, and USB drives
- *File*—it is possible to protect sensitive information by encrypting files and then transferring the encrypted file by posting to web sites, ftp servers, as e-mail attachments, or on transfer media such as CD-ROM, DVD-ROM, or USB flash-ROM ("thumb drive") devices. When using this method, it is not necessary to use encrypted e-mail because the file remains encrypted whether or not attached to the e-mail.
- *Data Transmission* – this type of encryption protects sensitive data as it passes over the public Internet or over private intranet and local area networks.

Policy and Procedures defines the organization's requirements for managing safety, system effectiveness, and security. To ensure processes and actions intended to reduce the overall risk to organizational assets and networks, implement industry accepted best practices and protocols within an organization.

Again, while this list cannot be considered exhaustive, each and every one of these measures is highly recommended for even the most basic user, system, or network. Employing none of the above measures would be considered high risk behavior. Without any of these measures in place, a system or network is sure to be at the highest level of risk and cannot be considered secure. The varied measures are necessary to compensate for the threats and vulnerabilities that apply to the multiple types of cyber

infrastructure in the healthcare sector. The former will be discussed in greater detail in the following section.

3.0 Cyber Vulnerabilities and Threats

In July of 2009 the FBI arrested a 25 year old contract security guard at a hospital in Dallas, Texas, for hacking the hospital's computers and air conditioning system. According to court documents, hospital officials had experienced problems with their heating, ventilation and air-conditioning (HVAC) units and were perplexed why none of the system alarms had gone off as programmed.[6] The hacker had posted videos showing him installing malware on hospital computers that made them part of a botnet he operated remotely. The images showed the HVAC control window for the hospital's surgery unit where an alarm setting was turned to "inactive." For many businesses, an attack on ventilation systems might be an inconvenience, but the threat could be much more serious for critical care patients in healthcare facilities. The hacker's intrusion into hospital systems was allegedly made in preparation for a larger denial of service attack on July 4th.[7]

Technological and security system advancements have led to more advanced and adaptive cyber attacks. Those adaptations include measures to bypass current technological countermeasures or take advantage of the human element of cybersecurity, such as using social engineering techniques and timing incidents to occur when IT professionals are already distracted, such as during natural hazards and other events.[8] The risk also includes a rising number of zero-day vulnerabilities – flaws in software code discovered before a fix or patch is available – combined with a steady increase in the number of individuals capable of exploiting the vulnerabilities and the near-static average time for developing security patches.[9]

It is important to note that the information presented in this section is not intended to be a comprehensive depiction of all of the risks posed to your particular system; an individual risk assessment would be necessary to gain that level of insight. All readers are encouraged to put their systems through a rigorous risk assessment to determine an individual facility, network, or system's risk.

---

[6] Helmer, Gabriel M., Security, Privacy and the Law., *Incident of the Week: FBI Arrests Hacker Posing as Security Guard Who Infiltrated Texas Hospital Days Before "Devil's Day" Attack*, July 2, 2009, available at http://www.securityprivacyandthelaw.com/2009/07/articles/cybersecurity-cyb...curity-guard-who-infiltrated-texas-hospital-days-before-devils-day-attack, accessed March 8, 2010.

[7] Goodin, Dan., The Register, ***Feds:*** *Hospital hacker's 'massive' DDoS averted: Arrest foils 'Devil's Day' scheme*, July 1, 2009, Available at http://www.theregister.co.uk/2009/07/01/hospital_hacker_arrested, accessed March 8, 2010.

[8] The SysAdmin, Audit, Network, Security (SANS) Institute, The Top Cyber Security Risks, September 2009, available at http://www.sans.org/top-cyber-security-risks/summary.php, accessed June 27, 2010.

[9] According to the SANS Institute, "zero-day exploits in client-side applications [are] one of the most significant threats to your network, and require that you put in place additional information security measures and controls to complement your vulnerability assessment and remediation activities." The Institute's Web site includes more than 25 vulnerabilities of medium or high severity that were identified one year ago or more, yet still do not have a fix or patch in place.

3.1 Common Cyber Threats

When hacking first became a problem in the 1980's and early 1990s, attackers had to be both skilled with, and knowledgeable about, systems they went after. It was often the case that the required skill of the hacker had to be substantial even to develop rudimentary attacks. Defenses were simple, and the software that hackers used for their attacks was not very sophisticated. Since the mid 90's, the cyber "arms race" has drastically changed the complexity of attacks. Networks now face some of the most complex code ever written. On top of that, attackers no longer have to be highly skilled because many of the best tools have been packaged into simple plug-and-play programs.[10]

The Department of Homeland Security's Critical Infrastructure Protection Cyber Security (CIP CS) Program collaborates with critical infrastructure sectors to assist industry stakeholders in securing their cyber systems. Throughout sector-specific and cross-sector collaborations, CIP CS has identified specific cyber threats that affect certain sectors, or have the potential to affect sectors in the future. The table below identifies some of the major cyber threats facing the HPH Sector. Keep in mind that the following threats are neither restrictive nor comprehensive.

Threat	**Description**[11]	**Example**
Insider Threat	Employees or trusted third parties who intentionally or unintentionally damage/destroy a system and/or steal data	An office cleaner at HealthSouth Ridgelake Hospital in Florida pled guilty in 2008 to fraud for ordering credit cards on the Internet with stolen patient personal information.[12]
Access Control Breaches (Physical Theft)	Malicious actors manipulate or bypass access control systems or procedures to gain unauthorized physical access to information or restricted/private sections of a facility	In April 2011, a laptop belonging to the Oklahoma State Department of Health was stolen from an employee's car. The laptop contained a database with hospital medical records of 35,000 children, and more than 133,000 patients were notified of the breach.[13]
Malware	Malware is employed to exploit sector cyber systems to destroy/disable systems	University Health Services of University of Massachusetts-Amherst had to notify patients in March 2011 of a potential breach

[10] Anderson, Robert. Powerpoint Presentation., Cyber Threats to Special Nuclear Material (SNM) Sites. Presented October 14-15, 2010. Idaho National Laboratory.

[11] For further information on cyber threats, please refer to the US-CERT Cyber Threat Descriptions at http://www.us-cert.gov/control_systems/csthreats.html and the F-Secure Threat Types at http://www.f-secure.com/en_EMEA-Labs/virus-encyclopedia/articles/classification/threat-types.html.

[12] Messmer, Ellen., PCWorld., *Are healthcare organizations under cyberattack?*, February 2007., available at http://www.pcworld.com/article/142926/are_healthcare_organizations_under_cyberattack.html, Accessed June 27, 2010

[13] Anderson, Howard., Healthcare Info Security., *Laptop stolen from car leads to breach.* April 2011., available at http://www.healthcareinfosecurity.com/articles.php?art_id=3541, Accessed April 30,2011

	and/or steal data	of their health information. A UMass workstation was inadvertently infected with a malware program in June 2010 and was not corrected until October 2010.[14]
Network Breaches	Outside actors gain unauthorized access and manipulate legitimate programs or install malicious ones to execute a variety of functions	A former security guard at a Dallas hospital pled guilty in May 2010 to two counts of transmitting malicious code for hacking into his employer's computers while working the night shift, which was part of a modest botnet intended to rival other hacker gangs.[15]

[14] Oh, Jamie., Beckers Hospital Review., *UMass Amherst data breach affects 942 patients*. March 10, 2011 available at http://www.beckershospitalreview.com, Accessed May 18, 2011

[15] Reeder, Kara., IT Business Edge., *Security guard enters guilty plea after hacking employer's computers.* March 17, 2010., available at http://www.itbusinessedge.com/cm/community/news/sec/blog/security-gaurd-enters-guilty-plea-for-hacking-employers-computers/?cs=41199, Accessed June 27, 2010.

3.2 Common Cyber Vulnerabilities & Consequences

There are numerous vulnerabilities in the cyber domain. These vulnerabilities span from the extremely basic to the extremely technical. The table below shows common cyber vulnerabilities and their associated impacts.

Security Risks	Threat	Vulnerability	Immediate Consequence	Cascading Consequence	Mitigation
Availability Loss	• Botnets • Cross-Site Scripting • Distributed Denial of Service (DDoS) • Insider • Natural disaster • Power failure • Terrorism • SQL Injection	• Lack of antivirus protection • Lack of intrusion protection/ prevention • Lack of redundancy and recoverability • Patch management	• Loss of HPH services • Patient errors • Unnecessary duplication of tests, etc.	• Financial losses • Loss of brand / reputation • Loss of life	• Intrusion prevention/ detection • Anti-virus software • Redundant / failover systems • Warm back up sites • Multi-factor authentication • Data encryption • Auditing • Least privilege • Background investigations • Hardware lock down • Break glass mode
Confidentiality Loss	• Botnets • Hacking • Insider • Malware • Phishing • SQL Injection	• Inadequate Patch management • Inadequate Configuration management • Inadequate password management	• Data loss • Data Theft	• Blackmail • Civil Suits • Financial insolvency • Financial theft • Fraud • Identity theft • Loss of Brand	• Multi-factor Authentication • Identity management • Data transport Encryption • Auditing across domains
Integrity Loss	• Botnets • Buffer Overflows • Cross-Site Scripting • Hacking • Insider • Malware	• Inadequate Patch management • Inadequate Configuration management • Inadequate password management Lack of anti-virus software • Software vulnerabilities	• Data destruction • Data corruption • Inability to use patient data • Patient errors • Repudiation	• Loss of life • Loss of services • Recovery Service fees • Forensic service fees • Loss of Brand reputation • Civil Suits • Financial insolvency	• Auditing across domains • Data at rest encryption • Identity management • Multi-factor authentication • Secure hash and signatures • Transport layer encryption

Privacy Loss	• Accidental Disclosure
	• Hacking
	• Inappropriate authorization based on patient preference
	• Insider
		• Configuration management
		• Hosting PII and personal productivity tools (email, IM) on the same system.
		• Open USB ports
		• Open DVD/CD R/W drives
		• Patch management
		• Workstation configuration
			• Identity theft
			• Leakage of personally identifying information
				• Civil Suits
				• Financial insolvency
				• Fraud (medical and financial)
				• Identity theft
				  ○ Monetary loss
				  ○ Psychological
				  ○ Social
				• Loss of Brand
					• Auditing
					• Background investigations
					• Data encryption
					• Hardware lock down
					• Least privilege
					• Multi-factor authentication
					• PII detection tools

4.0 Managing Risk

There are a number of measures that organization can implement to successfully manage risks. As briefly discussed in Chapter 2, commonly recognized security practices include, but are not limited to:

- Identification and Authentication;
- Security Patch Management;
- Firewalls;
- Encryption; and
- Standardized Policies and Procedures.

This section further details these security practices, highlights any relevant regulatory requirements, and maps each security practice to the kinds of risks each security practice is designed to impact. Again, the information presented here is not intended to be a comprehensive depiction of all of the risk management techniques needed to secure every individual system; for that purpose individual risk assessments are recommended.

Identification and Authentication

Identification and authentication techniques provide owners and operators with a mechanism to identify system users as well as confirm that information is from a trusted source. These techniques help distinguish between those who are approved to access your system versus those who may or may not have malicious intentions. Identification and authentication can help prevent: intrusion into your cyber systems, loss of private information, and loss of availability of services.

Robust identification and authentication techniques are especially important in healthcare and public health. In many fields, practitioners collect sensitive data from a variety of sources, including patients, vendors, laboratory networks and so on. In order to protect that data a solid security policy should be in place requiring those with access to authenticate their identities. Figure A details the varying types of authentication techniques that may be employed.

Figure A: Authentication Types

Low Security – Single-factor authentication: Users create an ID and Password

Medium Security – Two-factor authentication: Presentation of two types of evidence, such as a password with a secure-ID token

High Security – Multifactor authentication: Presentation of at least three types of evidence, such as a Smartcard with a password and biometric evidence (such as fingerprints)

High-security for application and system transactions such as a file transport—two- way SSL

HPH stakeholders should always be aware of the impact the human threat element may have upon these security practices. For example, a Palmetto Florida woman hacked into the Suncoast Community Health Centers causing $17,000 worth of damage.[16] The woman, a former employee, hacked into the computer system and "deleted and moved files, changed administrative account names and passwords, removed access to infrastructure systems, changed pay and accrued leave rates on the employee payroll system and compromised the firewall used to protect the health centers' computer network." Be aware of disgruntled employees, both past and present, by keeping your systems updated. Require a password

[16] The Bradenton Herald. *Florida woman sentenced for hacking computer system.* December 2010. Available at: http://securityinfowatch.com/nod/1318798, Accessed on May 24, 2011

change and change access codes frequently. This will make it harder for individuals to bypass your security methods.

Relevant Regulation:

- Health Insurance and Portability and Accountability Act, Security Rule;
- Federal Information Security Management Act;
- The Office of Management and Budget (OMB) M-04-04, E-Authentication Guidance for Federal Agencies

Security Patch Management (SPM)

It is important to update your software package to fix any preexisting bugs or vulnerabilities. SPM is used to reduce the risk of compromise to applications, systems, and computers as a result of system flaws. The update should come directly from the software company in order to reduce the risk of further corruption. Pre-programmed medical devices are at high risk for issues after experiencing a security patch update. According to Lynn Sherrill, the deputy director of The Department of Veterans Affairs health information security division, 173 medical devices have been infected with malware since January 2009. Be aware that some medical devices can become degraded or compromised from a security patch; therefore patches should be thoroughly analyzed, tested, and prioritized before use. If the software patch affects the safety or effectiveness of a medical device, you should report that information to the FDA.[17]

Relevant Regulation:

- Federal Information Security Management Act of 2002
- Health Insurance Portability and Accountability Act, Security Rule of 2003

Firewalls

Firewalls permit authorized users access to your computers network system. Using built-in filters, firewalls block potentially dangerous material from entering your network while logging attempted intrusions. The biggest danger to your firewall is the public internet. There are four different methods used by firewalls to restrict network traffic: packet filtering, circuit-level gateway, proxy server, and application gateway. Packet filtering limits the flow of information based on rules created by the systems administrator. The packet filter will analyze the headers on incoming and outgoing packets. Packets are then either allowed or denied based on the source of the information; the packets intended destination, and/or the type of port used.

Did you know? In January of 2011 a hacker was able to attack the website and Internet domain belonging to the United States Department of Defense prescription drug database. The site manages national pharmaceutical contracts for The Department of Defense as well as The Department of Veterans Affairs. The hacker was able to access information describing the types of drugs that can be prescribed to active-duty military personnel, retirees and their families. The hacker was offering full control and root access to the site's domain for just $399!

Circuit-level gateways do not filter each individual packet but are useful for protecting the security of

[17] Anderson, Howard., Healthcare Info Security. Medical Device Security Raises Concerns. May 17, 2011. Available at http://www.healthcareinfosecurity.com/articles.php?art_id=3644, Accessed June 9, 2011.

your private network by preventing the exposure of your protected information. Circuit-level gateways apply security mechanisms when a Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) connection is established. Both TCP and UDP connections are the basic communication language or protocol of the Internet. Once the connection has been made, packets can flow between the hosts without further checking. Proxy Servers act as an intermediary between a user and the Internet. This ensures security, administrative control, and caching service. The proxy server is a part of a gateway server that separates your internal network from other external networks; and a firewall server that protects your network from outside intrusion. Figure B details firewall types.

Relevant Regulation

- Federal Information Security Management Act of 2002

Figure B: Types of Firewalls

Circuit Level - These firewalls monitor transmission control protocol (TCP) sessions to make certain they are legitimate. Circuit level firewalls hide the network from the outside.

Application Level - This type of firewall can be used to examine application data moving through the filter in order to make decisions about the intent of the data. It prevents malicious behavior and may also protect against spam, viruses, and access to undesirable websites.

Network Level - Typically designed into network appliances such as routers, these firewalls inspect packet headers and filter traffic. Network level firewalls cannot validate user inputs or detect maliciously modified URL requests.

Stateless Firewalls - These are only used to monitor network traffic and restrict or block packets based on where they originated or other static values. This type of firewall is unaware of traffic patterns and data flow therefore it is unable to determine if a malicious packet is entering the system under the guise of expected information.

Stateful Firewalls - This type of firewall can watch traffic stream along the network from one end to the other. It recognizes communication paths and can implement various IP Security (IPSec) functions.

Application Level - This type of firewall can be used to examine application data moving through the filter in order to make decisions about the intent of the data. It prevents malicious behavior and may also protect against spam, viruses, and access to undesirable websites.

Encryption

Encryption is a method of protecting information by transforming it into code. Only those who have that specific code can access the information. Figure C discusses the two types of encryption; storage and file. It is important to review the different types of encryption in order to ensure that you are operating using secure practices for transferring and sharing sensitive files. A two-part study titled "How Strong Are Passwords Used to Protect Personal Health Information in Clinical Trials?" was recently published in the Journal of Medical Internet Research found that "the majority of passwords used to protect files are poorly constructed and easily cracked using commercial password recovery tools". The study was led by the Canada research chair in Electronic Health Information at the Children's Hospital of Easter Ontario (CHEO) Research Institute, Khaled El-Emam. El-Emam used commercial password recovery tools to decode fourteen out of fifteen sensitive files that were sent through e-mail. Thirteen out of the fourteen files contained sensitive information and identifying factors such as birth date and gender.[18]

Figure C: Types of Encryption

Storage - Applies to mobile devices, electronic media such as CD-ROMs and DVD-ROMs, containing sensitive data, laptops, desktop, servers where sensitive data is stored, and USB drives.

File - Refers to the transfer of encrypted files to websites, FTP servers, e-mail attachments, CD-ROM/DVD-ROM, and/or USB flash-ROM ("thumb drives").

The study also found that unencrypted patient information is being shared via e-mail or shared drives containing common passwords. This will put your clients at risk for identity theft. Figure D notes other useful methods of encryption.

[18] El Emam, Khaled, Journal of Medical Internet Research, How Strong are Passwords Used to Protect Personal Health Information in Clinical Trials? Available at http://www.jmir.org/2011/1/e18/, Accessed June 9, 2011.

Figure D: Other Methods of Encryption:

Secure Data Stream:

- *Secure File Transfer Service:* Individuals place sensitive data files in a controlled access website location, protected by encryption and HTTPS connection.
- *Transport Layer Security:* Encrypting data that is actively flowing throughout the network.

Secure E-mail:

- *Pretty-Good-Privacy (PGP):* A data encryption and decryption program that allows a user to encrypt and sign e-mails.
- *Public Key Infrastructure (PKI):* Provides the greatest amount of protection in terms of confidentiality, integrity, and non-repudiation. PKI protects the contents of an e-mail and any attachments. It is encrypted independent of the transmission stream and therefore cannot be read by anyone other than the sender and the addressed recipients. Both the recipients and the sender will need to have PKI certificates in order to use this type of encryption.
- *Instant Messaging File Transfer:* Chat conversations using a secure solution, such as Office Communicator, can be encrypted end-to-end. Such solutions should be used in a trusted and closed environment meaning these chats may only be viewed by the sender and receiver. This is particularly useful for transferring sensitive information your internal environment. The users identity can be confirmed before sending and a receipt confirming your information was receive will be sent immediately.

Wireless Encryption:

In certain situations wireless signals may radiate beyond the confines of your organization. Wireless technologies may include but are not limited to microwave, satellite, and Bluetooth. Wireless networks use authentication protocols which provide credential protection and mutual authentication. Within the field of medicine some related wireless technologies may include medications containing barcodes, telehealth systems, and communication devices such as radios or pagers.

Relevant Regulation

- Federal Information Security Management Act of 2002
- Health Insurance Portability and Accountability Act, Security Rule of 2003

Isolated Network

The process of separating computers and groups logically into manageable entities (Virtual Local Area Networks—LANs). LANs are computer networks that connect computers and devices in a limited geographical area such as your workplace or factory.

Relevant Regulation

- Federal Information Security Management Act of 2002

- Health Insurance Portability and Accountability Act, Security Rule of 2003[19]

Policy and Procedures:

Standardized policies and procedures should be implemented to identify your organization's requirements for managing safety, system effectiveness, and security. In March of 2011 Massachusetts General Hospital was forced to pay one-million dollars in legal fees and penalties due to the loss of 192 patient records. A hospital billing manager had taken paper records out of the hospital to work on them from home but accidentally left said paper records on an MBTA subway train. The records were never recovered. Since the incident, Massachusetts General Hospital has agreed to implement a "corrective action plan" (CAP) as well as pay to train its employees on the CAP.[20] Once a breach occurs, you should institute new policies regarding the use of paper documents, as well as the encryption of data on laptops and other portable devices. Policies and procedures should be audited at least once a year to make sure you are keeping up with the changes in legislation and technology.

Relevant Regulation

- Federal Information Security Management Act of 2002
- Health Insurance Portability and Accountability Act, Security Rule of 2003

[19] Legislation does not detail the need to isolate a network but both of the aforementioned legislations require that organizations ensure the confidentiality, integrity, and availability of information systems and the data residing on those systems.

[20] U.S. Department of Health and Human Services., Press Release. *Massachusetts General Hospital Fined $1million*. Available at: http://www.hhs.gov/news/press/2011pres/02/20110224b.html, Accessed April 14, 2011.

Educational Resources

This section provides additional resources for the reader to access training on cybersecurity. They are provided for the reader to continue education and training in the cybersecurity field.

The DISA Information Assurance Support Environment provides a variety of free, on-line IA education, training, and awareness programs. IA training helps to ensure that the privacy, reliability, and integrity of our information systems remain intact and secure. (http://iase.disa.mil/eta/)

DHS/FEMA Certified Cyber Security Training is available through the TEEX Domestic Preparedness Campus (http://www.teexwmdcampus.com/index.k2)

DHS/FEMA Cyberterrorism Defense Analysis Center (CDAC), a national counter-cyber terrorism training program, developed by technical personnel and managers who monitor and protect the nation's critical infrastructures, through their Cyberterrorism Defense Initiative (CDI), proves free classes to qualified personnel (state/local government, law enforcement, firefighters, public utilizes, public safety and health, emergency medical services, and colleges and universities). Classes are held free of charge to qualified personnel in easily accessible and centralized locations throughout the US. http://www.cyberterrorismcenter.org/

InfraGard Awareness Information Security Awareness Course is FREE to all individuals and small businesses with 50 or fewer employees. This training will help you and your employees understand how you to help make your workplace more secure. It will also teach you vital skills to protect yourself and your family from cybercrime and identity theft. (https://www.infragardawareness.com/index.php)

US Department of Defense (DoD) - Free web-based cyber training (Information Assurance (IA) covering a range of security topics. (http://iase.disa.mil/eta/online-catalog.html)

Texas Engineering Extension Service (TEEX) - formerly ACT Online Cybersecurity Training – This program is supported by the US Dept. of Homeland Security and the Federal Emergency Management Emergency Agency (FEMA). The program offers ten courses in three discipline-specific tracks: Non-Technical for End-Users; Technical for IT Professional; and Business Managers and Professionals. (http://www.teexwmdcampus.com/user_defined_content.k2?contentID=6)

The Center for Infrastructure Assurance and Security (CIAS) – University of Texas at San Antonio – CIAS is the operational division of the UTSA Institute for Cybersecurity Security and is designed to leverage its infrastructure assurance and security strengths as part of the solution to the nation's homeland security needs. (http://www.ciastraining.com/)

National Webcast Initiative – A collaborative effort between the US Department of Homeland Security's National Cyber Security Division and the Multi-State Information Sharing and Analysis Center as a means to provide timely and relevant cybersecurity education and information to a broad audience. Embracing the concept that security is everyone's responsibility, these webcasts are available to the public and free or charge. A number of vendors offer their services at no cost to help develop and deliver the webcasts. (http://msisac.cisecurity.org/webcast/)

SANS Webcasts – SANS Webcasts are live broadcasts that allow you to hear a knowledgeable speaker while viewing presentation slides that you download in advance. You need a Real Audio Player or Windows Media Player (free downloads are available on the webcast access page), and a SANS Portal account. If you do not have an account, go to the SANS Portal page and fill in the free registration form. Once you have an account, you can

also access an archive of past webcasts. http://www.sans.org/webcasts/ Archive: (http://www.sans.org/webcasts/archive/)

Stanford University – Via Stanford University's Entrepreneurship Corner website, a series of free video lectures on cybersecurity are provided. (http://ecorner.stanford.edu/authorMaterialInfo.html?mid=358)

References for Additional Information

This section provides links and resources for the reader to access further information on cybersecurity.

Website Resources

United States Computer Emergency Readiness Team (US CERT): US-CERT's mission is to improve the nation's cybersecurity posture, coordinate cyber information sharing and proactively manage cyber risks to the nation while protecting the constitutional rights of Americans. (http://www.us-cert.gov/cas/tips/)

Build Security In (Software Assurance): Contains tools, guidelines, and other resources for security practitioners and software developers to build security into the software development process (buildsecurityin.us-cert.gov)

Homeland Security Information Network for Healthcare and Public Health: The Homeland Security Information Network for the Healthcare and Public Health community (HSIN-HPH) is the nation's primary web portal for public / private collaboration to protect its critical infrastructure and resources. Cyber resources include HPH-specific items in the Cyber Open-Source Cyber Digest. To request access to HSIN-HPH, please visit https://connect.hsin.gov/hph/event/registration.html and complete the online application.

Daily Open Source Infrastructure Report (OSIR): The Department of Homeland Security's Daily OSIR is collected each business day as a summary of open-source published information concerning significant critical infrastructure issues. (http://www.dhs.gov/files/programs/editorial_0542.shtm)

National Security Agency (NSA): The NSA provides fact sheets for information assurance and security. (http://www.nsa.gov/ia/guidance/security_configuration_guides/fact_sheets.shtml)

National Institute of Standards and Technology (NIST) Computer Security Division provides a number of useful resources regarding cyber and information security. (http://csrc.nist.gov)

National Vulnerability Database: Repository of vulnerability management, security measurement, and compliance information. nvd.nist.gov

OnGuard Online: Offers practical tips to protect against Internet fraud, to secure personal computers, and to protect personal information. www.onguardonline.gov

Federal Trade Commission: Provides resources for protecting consumers from predatory business practices, including online scams and identity theft (www.ftc.gov)

Articles

Ponemon Institute and Imprivata: How Single Sign-On is Changing Healthcare. A new research report from the Ponemon Institute and Imprivata on the use of single sign-on (SSO) technology shows that the average clinician spends 122 hours a year (3 weeks) trying to access various forms of electronic medical records (EMR). This is caused by the overabundance of passwords and logins being managed to access the applications needed for accessing patient care. According to the national study, SSO technology can dramatically decrease the amount of time clinicians spend on the access process. More than 400 healthcare IT representatives and clinicians responded to the survey.

McAfee and the Center for Strategic and International Studies: In the Dark: Critical Department of Homeland Security Industries Confront Cyber attacks. Cyber-attacks on critical infrastructure companies are on the rise, with a jump in extortion attempts and malware designed to sabotage systems, like Stuxnet, according to a new report from McAfee.

Redspin: Breach Report 2010 reports**.** A total of 225 breaches of patient health information have occurred since the interim final rule on breach notifications was issued in August 2009 as part of the HITECH Act.

Deloitte: Privacy and Security in Health Care: A Fresh Look**.** Health care organizations using advanced technologies are at increasing risk for patient data breaches. The report said as the health care industry increasingly adopts electronic health records, clinical data warehousing, home monitoring, and telemedicine, the risks of patient data breaches are also increasing.

Ponemon Institute and Informatica Corporation: Health Data at Risk in Development: A Call for Data Masking**.** Serious risks to patient data exist in the development and testing of healthcare software, according to a survey. The report calls for data masking in order to mitigate this risk.

Journal of Medical Internet Research: How strong are passwords used to protect personal health information in clinical trials? Privacy and security safeguards designed to protect patients' sensitive files during clinical trials are inadequate. Researchers were able to crack the passwords for 93 percent (14/15) of password-protected files transmit-ted by email during regulated Canadian clinical trials

Condensed Glossary of Cyber Terms

Add-on Software (Adware): Software which automatically plays, displays, or downloads advertising material onto your computer once the application has been installed or is in use.

Authentication: The act of confirming the identity of a user and/or verifying that a program, e-mail, electronic signature, etc. is from a trusted source.

Bandwidth: The capacity of a communication channel to pass data throughout the channel in a given amount of time, expressed in bits per second (bps).

Backdoor: Gaining unauthorized access to a program, online service or an entire computer system without detection or documentation.

Business Systems: Mission essential systems that are used to manage or support common business processes such as Enterprise Resource Planning, E-commerce, and E-mail systems.

Control Systems: Cyber systems used to monitor and control sensitive processes and physical functions including SCADA (*see below for definition*), Process Control Systems (*HVAC*), and Distributed Control Systems (*Environmental Control Systems*).

Cookie: Data exchanged between an HTTP server and a web browser (i.e. Internet Explorer or Firefox) to store state information on the client side and retrieve it later for server use.

Cyber Crime: Criminal activities that use computers and/or networks.

Cyber Infrastructure: Physical assets and virtual systems and networks that enable key capabilities and services.

Cyber Security: Protection of information from theft or corruption, or the preservation of availability, whole allowing the information and property to remain accessible and productive to its intended users.

Cyberspace: An environment in which digitized information is distributed on networks of computers.

Data Driven Attack: A form of attack that is encoded in seemingly innocuous data, which is executed by a user or a process to implement an attack. This is a concern for those depending solely on firewalls because the attack is able to penetrate the firewall in data form and then launch a system attack.

DDoS: Distributed Denial of Service; Flooding the networks or servers of individuals or organizations with false data requests so they are unable to respond to requests from legitimate users.

Dictionary Attacks: An attack that uses a brute-force technique of successively trying all the words in some large, exhaustive list.

Domain: A sphere of knowledge, or a collection of facts about some program entities or a number of

network points or addresses, identified by a name. On the Internet, a domain consists of a set of network addresses. In the Internet's domain name system, a domain is a name with which name server records are associated that describe sub-domains or host. In Windows NT and Windows 2000, a domain is a set of network resources (applications, printers, and so forth) for a group of users. The user need only to log in to the domain to gain access to the resources, which may be located on a number of different servers in the network.

Domain Hijacking: Domain hijacking is an attack by which an attacker takes over a domain by first blocking access to the domain's DNS server and then putting his own server up in its place.

Domain Name Systems (DNS): The way that Internet domain names are located and translated into an Internet Protocol addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

Encryption: A method of protecting information by transforming it into code. Only those who have that specific code can access the information. There are two types; storage and file. Storage refers to mobile devices, electronic media, laptops, desktop, servers where sensitive data is stored and USB drives. File refers to encrypting files and then transferring the encrypted file by posting to web sites, ftp servers, as e-mail attachments, or on transfer media such as CD-ROM, DVD-ROM, or USB flash-ROM devices.

Ethernet: A system for connecting a number of computer systems to form a local area network, with protocols to control the passing of information and to avoid simultaneous transmission by two or more systems

Fault Line Attacks: Using weaknesses between interfaces of systems to exploit gaps in coverage.

Filter: A filter is used to specify which packets will or will not be used. It can be used in sniffers to determine which packets get displayed, or by firewalls to determine which packets get blocked.

Firewall: A firewall is a hardware or software solution to enforce security policies. From a physical perspective, a firewall is equivalent to a lock on a door. It permits only authorized users such as those with a key or access card to enter. A firewall has built-in filters that block unauthorized or potentially dangerous material from entering the system. It also logs attempted intrusions. They manage the traffic entering and leaving a network by applying any of four different mechanisms to restrict traffic—packet filtering, circuit-level gateway, proxy server, and application gateway. The packet filtering allows the firewall to perform packet inspections to ensure that the data entering your infrastructure is safe. Organizations can develop business rules to limit what is allowed in or out. Firewalls are best utilized either at the perimeter of the network or between the network and infrastructure and the Internet.

Gateway: A network point that acts as an entrance to another network.

GCC: Government Coordinating Council

Hacker: A person with special expertise in computer systems and software. There is no illegality involved with being a hacker; this is the difference between a hacker and a cracker.

Hardening: Hardening is the process of identifying and fixing vulnerabilities on a system.

Host: Any computer that has full two-way access to other computers on the Internet. Or a computer with a web server that serves the pages for one or more Web sites.

Hybrid Encryption: An application of cryptography that combines two or more encryption algorithms, particularly a combination of symmetric and asymmetric encryption.

Identitity Management: A method of validating a person's identity when he/she tries to access a network.

Incident Handling: Incident Handling is an action plan for dealing with intrusions, cyber-theft, denial of service, fire, floods, and other security-related events. It is comprised of a six step process: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.

Incident Management: Executing a defensive response when a network's security is threatened.

Information Technology (IT): Hardware, software, and IT systems and services, including development, integration, operations, communications, and security that support cyber infrastructure.

Integrity: Integrity is the need to ensure that information has not been changed accidentally or deliberately, and that it is accurate and complete.

Internet: A term to describe connecting multiple separate networks together.

Internet Protocol (IP): The method or protocol by which data is sent from one computer to another on the Internet.

Intranet: A computer network, especially one based on Internet technology, that an organization uses for its own internal, and usually private, purposes and that is closed to outsiders.

Intrusion: Unauthorized act of bypassing the security mechanisms of a system.

Intrusion Detection: A security management system for computers and networks. An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

IP Address: A computer's inter-network address that is assigned for use by the Internet Protocol and other protocols. An IP version 4 address is written as a series of four 8-bit numbers separated by periods.

IP Spoofing: The technique of supplying a false IP address.

Keylogging: a method of capturing and recording user keystrokes.

List Based Access Control: Associates a list of users and their privileges with each object.

Malware/Malicious Code: Malicious Software designed to infiltrate a computer system without the owner's informed consent. Any code that can be used to attack a computer by spreading viruses, crashing networks, gathering intelligence, corrupting data, distributing misinformation and interfering with military or civilian operations including navigation, transportation, logistics, communications and command and control

National Institute of Standards and Technology (NIST): A unit of the US Commerce Department. Formerly known as the National Bureau of Standards, NIST promotes and maintains measurement standards. It also has active programs for encouraging and assisting industry and science to develop and use these standards.

PAP: Password Authentication Protocol is a simple, weak authentication mechanism where a user enters the password and it is then sent across the network, usually in the clear

Patch: An update to a system or software package as a code that is deployed into software in order to fix a bug or vulnerability. A small update released by a software manufacturer to fix bugs in existing programs.

Penetration: Gaining unauthorized logical access to sensitive data by circumventing a system's protections.

Proxy Server: A server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. A proxy server is associated with or part of a gateway server that separates the enterprise network from the outside network and a firewall server that protects the enterprise network from outside intrusion.

Risk Management: Identifying vulnerabilities in a network and developing a strategy to protect against an attack.

Role Based Access Control: Role based access control assigns users to roles based on their organizational functions and determines authorization based on those roles.

SCC: (1) Secretary's Command Center; (2) Sector Coordinating Council

Secure: Safe from penetration or interception by unauthorized persons

Secure Shell: A program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another.

Secure Sockets Layer: A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection.

Security Patch Management: Updating software to reduce the risk of compromise to applications, systems, and computers as a result of system flaws.

Sensitive: Work, duties, or information of a highly secret or delicate nature, especially within government

Sensitive Information: Sensitive information, as defined by the federal government, is any unclassified information that, if compromised, could adversely affect the national interest or conduct of federal initiatives.

Server: A computer set up to provide information on request via a network.

Session: a virtual connection between two hosts by which network traffic is passed.

Session Hijacking: Take over a session that someone else has established.

Session Key: In the context of symmetric encryption, a key that is temporary or is used for a relatively short period of time. Usually, a session key is used for a defined period of communication between two computers, such as for the duration of a single connection or transaction set, or the key is used in an application that protects relatively large amounts of data and, therefore, needs to be re-keyed frequently.

System Security Officer (SSO): A person responsible for enforcement or administration of the security policy that applies to the system.

Tamper: To deliberately alter a system's logic, data, or control information to cause the system to perform unauthorized functions or services.

TCP/IP: A synonym for "Internet Protocol Suite;" in which the Transmission Control Protocol and the Internet Protocol are important parts. TCP/IP is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an Intranet or an Extranet).

Threat: Any circumstance or event with the potential to adversely impact an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.

Threat Model: A threat model is used to describe a given threat and the harm it could to do a system if it has a vulnerability.

Threat Vector: The method a threat uses to get to the target.

Trojan Horse: A code which masks itself as a useful program and when activated, it performs malicious activity such as locating protected passwords or damaging data on a computer’s hard disk.

User Contingency Plan: User contingency plan is the alternative methods of continuing business operations if IT systems are unavailable.

Virus: A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting - i.e., inserting a copy of itself into and becoming part of - another program. A virus cannot

run by itself; it requires that its host program be run to make the virus active.

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited.

Worm: a self-replicating computer program. It uses a network to send copies of itself to other nodes (computer terminals on the network) and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms almost always cause harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.