Global Journal of Computer Science and Technology
Network, Web & Security
Volume 13 Issue 3 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

It Security in Hospital Management

By Manoj Chopra
Bonnie Foi College

Abstract - Hospital IT security presents many unique challenges that must be solved by the entire organization. Network and computer threats can cause thousands of dollars in lost time and resources, legal repercussions, and damaged reputation. Despite warnings from a wealth of public breach notifications, many hospitals are inadequately prepared to deal with today's computer-based attacks. This research explores the root causes of hospital network and computer in security, and addresses these problems with methods implemented in actual hospitals. A lack of comprehension of methods to assess and implement security measures by hospital IT security employees can hinder network visibility and prevent their ability to stop threats. In addition, these same people are unable to express security concerns in terms management can understand, harming their credibility within the business as a whole. Without this support, organizational change is impossible. By addressing these concerns with a combination of people, process, and tools, we can solve complex problems, protect patient data, and ensure IT operations so hospitals can serve their community and save lives.

Keywords : *web filtering, e-mail filtering, system patching, antivirus, secure wireless access, firewall configuration.*

GJCST-E Classification : *K.6.5*

Strictly as per the compliance and regulations of:

It Security in Hospital Management

Manoj Chopra

Abstract - Hospital IT security presents many unique challenges that must be solved by the entire organization. Network and computer threats can cause thousands of dollars in lost time and resources, legal repercussions, and damaged reputation. Despite warnings from a wealth of public breach notifications, many hospitals are inadequately prepared to deal with today's computer-based attacks. This research explores the root causes of hospital network and computer in security, and addresses these problems with methods implemented in actual hospitals. A lack of comprehension of methods to assess and implement security measures by hospital IT security employees can hinder network visibility and prevent their ability to stop threats. In addition, these same people are unable to express security concerns in terms management can understand, harming their credibility within the business as a whole. Without this sup- port, organizational change is impossible. By addressing these concerns with a combination of people, process, and tools, we can solve complex problems, protect patient data, and ensure IT operations so hospitals can serve their community and save lives.

Keywords : web filtering, e-mail filtering, system patching, antivirus, secure wireless access, firewall configuration.

I. Introduction

Securing a hospital network is challenging. Doctors and physicians often require special needs, and external vendor systems require agreements that pose restrictions on possible security controls. In addition, hospitals have many of the same challenges other organizations struggle with. Improper management of systems and network defenses can expose private information and credit card numbers to attackers. This can violate laws and regulations, cause negative publicity, impact the financial stability of the business, and hinder the ability to provide care to patients.

Effective security requires many working parts in an organization, not all of which are technical solutions. Defined process, skilled and well-managed personnel, and management support are vital aspects of security. Many hospitals fail to address one or more of these aspects, leaving their network open from multiple attack vectors.

Security breaches may also hinder a hospital's ability to adequately care for its patients, or admit new patients. Viruses and other attacks can cause medical record systems to be disabled, forcing hospitals to revert to a paper system and decreasing efficiency. In some cases, incidents can prevent hospitals from providing adequate care. In these cases, ambulances may have to be rerouted to other medical facilities in the area, losing business and endangering those who need immediate care.

Author : Computer Science Department.
E-mail : Manoj_19143@ rediffmail.com

II. Defining 'Security'

First, when we refer to 'security' throughout this research paper, we are referencing IT security, not physical or some other type. Security is often defined as protecting the confidentiality, integrity, and availability of data, but the interpretation and context of these aspects will change from organization to organization.

Rather than creating an overall definition of 'security', we will define it in terms of several goals. When we refer to 'security' throughout this paper, we will mean technology, processes, procedures, and organizational structures that:

- Ensure the confidentiality, availability and integrity of electronic/digitized assets and data, especially PHI.
- Ensure the ability to provide quality care to hospital patients through the use of technology.
- Minimize the impact of security threats against the needs of the business.

We hope to represent the flexible and intangible nature of security, especially in a hospital environment, by defining 'security' as a collection of goals, rather than an absolute state. As we will show later, security events can be quantified in terms of risk, which must either be accepted or not for each hospital dependent on individual tolerance. Some hospitals may accept more risk while defining themselves as 'secure', while others will accept less risk. It is not a term that can be absolutely defined, and we make no attempt to represent it as such. We simply present one useful definition for our purposes here.

III. Proposal

Many approaches to network and computer security focus purely on better technology. By increasing the effectiveness of anti-virus, web proxies, intrusion detection, and other technologies, attacks can theoretically be prevented over the network. In reality, this is not the case. The true problem of network and computer security in hospitals is not with the current technology solutions available on the market. The problem is with the way security is understood, accepted, and implemented by the people within the hospital. Communication between security teams and

upper-level management is a driving factor for this problem. As we will show, management support is required for any major change in an organization, because many security changes affect the entire organization. If this support is missing, many changes are ineffective or incomplete. Our approach seeks to address both the technical issues as well as communication issues. It meets the needs of the organization while defending its most important assets. It provides the flexibility and resiliency to cope with the changing world of computer and network security, and addresses the complex factors involved in security for a large organization. Our method contains multiple stages. First, hospitals must understand the specific challenges they face. Next, specific methods will be used for assessing a hospital's security and risk posture. Once these are complete, other methods can be used to consistently improve IT security in these organizations. In the final section, case studies will illustrate the success of the method. It was implemented in several hospitals who have all reached various levels of maturity.

IV. Hospital Security

a) *Implementation*

As discussed previously, security within an organization is a combination of people, process, and tools. Technical controls - tools - provide a means to restrict and regulate the network. Process defines standards by which the organization implements and enforces security controls. Finally, the people, including politics between departments, the culture of the organization, and simply their communication, are ultimately responsible for security. All three are necessary to protect the hospital network. The assessment phase helps the hospital understand its current security posture. Using the data obtained, security exposures can be identified, and then corrected. The methods described in this chapter include many specific technical controls that must be implemented to provide a reasonable degree of security. Beyond these controls, most hospitals struggle with communication and internal politics. Lower level security employees cannot communicate appropriately with upper level management, which will allow them to obtain the support they need for security initiatives.

V. Specific Technical Controls

Every hospital must have a set of technical controls to protect their network. They must also have the proper personnel and management support to drive the change necessary to implement and enforce the controls. A list of controls have been defined below that will drastically improve security for most hospitals. Each of these controls can be implemented in many ways. No particular vendor or implementation is recommended, although several are mentioned as examples. These are details that must be worked out for each individual hospital to solve their specific needs.

a) *Web Filtering*

The majority of successful attacks today expose vulnerabilities in web browsers. These can be attacks against the browser itself (such as Internet Explorer or Mozilla Firefox), but they can also exploit other services utilized by the browser such as Java or Adobe Flash. As such, normal web browsing creates a large security risk for any hospital. To help protect against these specific attacks, web filtering appliances can be purchased from many vendors. It is also possible to use an open source tool, such as Snort, to create a custom web filter, but most organizations opt to purchase a pre-built solution.

Control 1: All web browser traffic must be filtered through a web gateway or proxy appliance.

Web filters generally work using blacklists. This approach blocks specific web traffic based on content signatures, DNS name, IP address, or other static rules. Any traffic that does not specifically match is allowed by default. Some web filters act as an enterprise-wide anti-virus solution. For example, McAfee's Web Gateway[19] searches for content matching known viruses. Due to the prominence of attacks originating from web browsing, a web filter is absolutely necessary for any hospital.

b) *Email Filtering*

The primary responsibility of an email filter is often to reduce or eliminate spam for an organization, and minimize viruses and other threats. Email attacks can trick a user into opening a malicious web link or attachment, but they can also attempt to get a user to divulge sensitive information. To prevent most spam and malicious emails, we can use a dedicated email filter, such as Cisco IronPort[9].

Control 2: All email must be filtered through a dedicated email server to remove spam and malicious attachments.

Like the web filter, this approach may not prevent all attacks, but we can use it to help reduce the attack surface of the organization.

c) *System Patching*

Most virus-related incidents in hospitals can be prevented with effective patch management. Most hospitals have thousands of computing devices on their network, a large percentage of which are running some version of Microsoft Windows. Many security vulnerabilities are discovered each month for Windows that can allow an attacker to successfully exploit and compromise a system. Because new vulnerabilities are discovered at a high rate, it becomes equally important

that we are able to apply patches that correct these vulnerabilities. Figure 4.1.3 shows the number of vulnerabilities released per month for Microsoft products that were rated `Consistent Exploit Code Likely' by their Exploitability Index [20]. This rating means\analysis has shown that exploit code could be created in such a way that an attacker could consistently exploit that vulnerability."[20] Also included is a tally of those vulnerabilities that were being actively exploited on the Internet at the time Microsoft released the monthly bulletin announcing the vulnerabilities. [21] This measurement shows that sometimes a vulnerability is being exploited before a patch is even available. This increases the urgency for applying a patch to vulnerable systems.

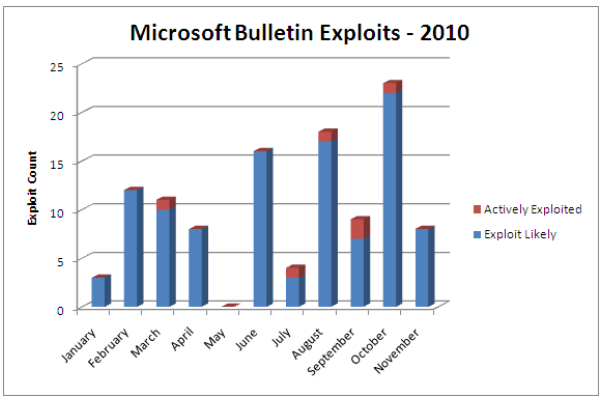

Figure 1 : Microsoft Bulletin - Count of likely exploitable vulnerabilities per month in 2010

Control 3: Automatic patching must be implemented and enforced for all computer systems on the network. Sensitive systems or systems that cannot utilize an automatic system must have a patching procedure in place.

Microsoft Windows is not the only attack surface that requires regular patching. Adobe products (Flash, Acrobat Reader, Shockwave, etc.), Java, Apple Quicktime, and any other popular software are often discovered to have severe security vulnerabilities as well. Other operating systems, such as many Linux variants or Mac OS X release patches for newly discovered security vulnerabilities, although these are exploited less often due to a smaller user base. Finally, many medical system vendors prohibit hospitals from installing patches on their computer systems, even if the hospital owns the system. They instead require the hospital wait for the vendor to patch the system for new vulnerabilities. Unfortunately, many of these systems never get patched once they are installed in the hospital environment. To combat this, other controls must protect these systems, such as network segregation and strict policy surrounding their usage.

d) Anti-Virus

Anti-virus is primarily the last defense against an attack. When all other con- trols have failed, a local anti-virus installation can detect and block malicious code before it is able to compromise and infect a system. When referring to `anti-virus' in this paper, it should be considered a program which tries to detect and prevent any type of malicious attack on an end-point system. This can include Trojan Horses, viruses, worms, adware, spyware, and any type of attack normal enterprise anti-virus can detect and prevent. Anti-virus is most useful on Microsoft Windows computers. Solutions do exist for Linux and OS X, such as ClamAV[10] for Linux and Sophos[33] for OS X, but they typically provide less value to hospitals, who have a high number of Windows systems in the network environment.

Control 4: Anti-virus must be installed and up-to-date on end systems.

Anti-virus should be installed on any Microsoft Windows system with adequate resources. Administrators often forgo installing it on high load servers for fear it will adversely impact performance. This is a risk that can be accepted provided other controls protect the system. Like system patching, many medical system vendors prohibit hospitals from installing anti-virus solutions on their systems. Their reasons include performance concerns and unintended side effects. When this occurs, other controls must adequately protect these systems. The hospital should ensure that anti-virus is updated regularly to the latest software versions. This includes the anti-virus installation itself, but it also includes virus signatures released regularly from the vendor. This ensures the system can be protected from the latest known threats. Despite providing a valuable control, anti-virus is still limited by its signature definitions. It can only detect and protect a system from known threats. Polymorphic viruses and new attacks will bypass anti-virus and are still capable of compromising a system.

e) External Device Control

Any device capable of easily and physically carrying data inside or outside the hospital network can be classified as an \external device". This includes both hospital provided and personal laptops, and removable media such as USB ash drives or external hard drives. These devices can be connected to insecure networks outside of hospital control, which can cause them to become infected with a virus or other malicious software. Upon returning to the internal hospital network, the malicious code can then attack the internal network and company resources. Hospitals should also be concerned with data ex- filtration. A laptop is capable of carrying PHI outside the network, which can lead to a security incident if not adequately controlled.

Control 5 : Only hospital provided and controlled PCs should be allowed to connect to the internal network. USBs and other forms of removable media should be tightly controlled, and ideally completely restricted.

While company policy can provide some mitigation of this threat, it may not be a strong deterrent for many employees or other outside personnel (consultants, guests, etc.). Effective technical solutions tend to be expensive and difficult to implement. One example is Cisco's Network Access Control (NAC), which is certainly expensive, but when configured properly can protect against external devices.

Ideally, in the case of an external laptop or other computer, a technical solution will detect an attempt to connect to the network. It will then run through a series of checks before allowing the device to communicate with the rest of the network. These checks can include system patch levels, anti-virus installation and version, and other software checks. If the system passes, it is allowed to connect. If not, it must correct the problems before it can access the internal network. To correct the problems, a separate VLAN is often utilized to allow the user to download patches or other requirements. Software controls can be used to prevent users from using unauthorized external media. Super glue can also physically seal the USB drives of a computer, although we do not recommend this.

Laptops and other hospital resources (hard drives, USB sticks, etc.) carrying sensitive data must be fully encrypted if they can be taken outside hospital property. This is especially important for laptops or any device that may be a target for thieves. Many HITECH breach incidents[14] were related to stolen hard drives, USB sticks, or laptops containing personal data. In such cases, companies must disclose the data loss to the public, and then pay for remediation. With encryption, the only loss is the physical hardware.

Control 6: External devices storing sensitive data must be encrypted.

f) Secure Wireless Access

Wireless access points provide convenience for hospital employees and outside guests. The signal for access points is broadcast over the air, which can allow anyone within range to view and attempt to connect to the network. Without proper controls, an intruder could gain access to sensitive resources or disrupt network operations. Primarily, employee wireless access should be encrypted with enterprise WPA2 using a central RADIUS (Remote Authentication Dial In User Ser- vice) or AAA (Authentication, Authorization, Accounting) server. This provides a strong level of encryption and allows employee access to be controlled with a central server. Guest wireless access is typically unencrypted and open in most hospitals. This allows anyone, even attackers, to connect to the network. To prevent a malicious user from compromising the internal hospital network, the guest network should be on a completely separate network. Without restrictions on the guest wireless network, employees can also connect to this open network and bypass normal internal network filters (such as web filters or tight firewall rules). This can lead to employees accessing Internet resources that should be restricted. It is also possible external users can detect and attack an employee system connected in this way. To prevent this, WPA/WPA2 encryption should be enabled on the guest network, even if it uses a simple and publicly available encryption key. Employee systems should also be denied access to this network by using a network access control tool like Cisco NAC.

g) Firewall Configuration

Numerous resources exist explaining how to properly configure an enterprise firewall for security. This is only mentioned for posterity. Firewalls should be configured as restrictively as possible. Internal systems should not have unrestricted access to the external Internet. Direct access from the external Internet should be prohibited to the internal hospital network. A demilitarized zone (DMZ) should be designated for allowing external Internet access to resources hosted on the hospital network. The DMZ must be restricted from accessing the internal network.

Control 7: Firewalls should be properly configured to be as restrictive as possible.

VI. Other Controls

Most hospitals struggle to implement and maintain even basic controls, and the broad range of controls we listed above attempt to solve the most common areas of exposure. They should be implemented on any hospital network. However, many other controls should be used to provide more granular protections. As an example, passwords should be complex and changed regularly (as defined and accepted by company policy). This is a minor control that can be implemented with Microsoft Active Directory, and its definition can change per individual hospital. There are different ways to provide authorization to resources, such as Active Directory for network shares, or specific configurations for individual systems. Generally, users should be given minimal access to the resources they need to do their jobs. External Internet access should be restricted, internal server resources should be restricted, and individual workstation access should be restricted. By providing minimal access, we limit the exposure surface of the hospital computer and network resources. Technical controls help protect the hospital network. However, they are only one aspect of securing a network. The next section will discuss the

human aspect of security, which must be successful in order to meet the constantly changing security world.

VII. Security Personnel

The technical controls in the previous section provide strong protection against many forms of attack, but it is equally important to address the people side of security. Politics between differing groups and individuals, as well as the culture of the organization, play a role in security. Individual knowledge and skill are important as well. Hospitals are no different than any other organization in this manner. Low level security personnel are essential for implementing and maintaining security controls and providing creative solutions to problems. In addition, management must actively support and enforce security initiatives. The interaction between these groups has an effect on how security is implemented within the hospital. In this section, guidelines will be provided for structuring the security of a hospital. Also, when groups within an organization communicate effectively, they can solve security problems.

VIII. Security Team

The security team is tasked with administering and reviewing the security systems at the hospital. Not only do members of the security team configure and maintain appliances, systems, and security software throughout the organization, but they must also review logs and other reports for security incidents. They think and make decisions about security for the hospital, although final approval may defer to a manager or director. Members of the security team generally administer major security systems at the hospital such as firewalls, web filtering appliances, email and spam filters, IDS/IPS appliances, vulnerability scanning, central logging systems, anti-virus, and patch management systems. In many cases they will have other responsibilities that may or may not directly impact the security of the organization. Hospitals often do not have the resources to have dedicated security personnel without other responsibilities. In many cases, the members of the security team will not be directly responsible for administering a system that has an impact on security. This could be a weakness discovered from a vulnerability scan, a new web server that will be placed on the DMZ, or any number of IT operational items. When this occurs, members of the security team must work with other members of the organization to implement or maintain a system. They can provide advice on the security of the system, as well as test it to ensure it functions as intended. Good inter-departmental relationships are vital for this to be a success. When dealing with another department the security team will often rely on their manager or director. In some cases, a formal security team has not been established for the hospital. If this is the case, a security team should be created. When selecting team members, choosing personnel who already administer many of the devices and systems mentioned above can be a good idea. However, this selection is often decided by an already existing IT manager. The members must be trustworthy and reasonably knowledgeable about security. The team must also include a manager with the authority to make decisions acting the network infrastructure of the organization, and he or she must also be able to raise concerns with higher level management when necessary. When a team is established, they can begin to discuss and handle many of the responsibilities required of this team. Weekly meetings are often worth- while to ensure that everyone and the manager is on the same page. Formal policies must also be defined around this team and they must work with the organization to get these policies and responsibilities accepted. The security team is also responsible for thinking about and solving IT security problems for the hospital. Some problems may be directly solvable by members of the security team, while others must be delegated to outside groups through management. For example, a security team member may be directly responsible for the management of the hospital firewall, and can make any adjustments as necessary. This depends on the expertise of the individual team members. In some cases, the security team may only need to provide recommendations to other groups within the hospital. The security team should meet regularly, usually once per week. In each meeting the security team should assess the current state of computer and network security for the hospital, then address any new or ongoing initiatives. The team should always explore ways to improve the hospital's security, even if improvements are not forthcoming. It is then the manager's responsibility to best utilize the resources at his disposal and drive the initiatives of the security team.

IX. Management Support

Strong and efficacious network security begins with management support. The security manager oversees the security team and is responsible for ensuring resources are focused where necessary. This can be a balancing act between security responsibilities and normal IT responsibilities. The manager must also ensure that team members are consistently reviewing security data and reports so incidents are noticed and duly investigated. The security team must be supported further by an executive at the director or higher position (like Chief Information Security Oficer). The director must handle funding for the security program. They must also understand IT security risk and be able to present this effectively to the rest of the organization. Most importantly, they must help the security team navigate

the politics and culture of the entire hospital. Without support from the rest of the organization at a high level, the security team will be hindered during investigations and response, they will not be able to enforce policy, and they will not get proper funding. Management support is required to get the resources necessary, both in personnel and monetary, to efficiently and effectively deal with security problems. Their support is also needed for policy change and enforcement. "Those with the power to allocate resources, both financial and the time of employees, can control any change expressed from lower in the power structure.

Figure 2 : An example hospital organizational structure

X. Conclusion

Hospitals have many of the same IT security problems experienced by other organizations, but with added complications from doctors, external vendor systems, patient records, and specific legislation. They also struggle with insufficient resources and often lack comprehensive expertise to cover all areas of security. Ineffective communication between low level security personnel and management can cause misplaced priorities and misguided initiatives. Securing a hospital network requires a combination of technical controls, policies and processes, and responsibility among the people of the organization. By first understanding the hospital network and its resources, then by quantitatively measuring the IT security risk and understanding areas of exposure, a strong security strategy can be created and supported by management, the security team, and the rest of the organization. Finally, security must be continually assessed and reassessed. With new and innovative threats, effective security cannot remain stationary. It must constantly evolve to meet new challenges. IT security for hospitals cannot be solved with a simple approach and a single piece of technology. It is an entire process among many people within the organization. By addressing these problems as they are - complex and multi-tiered - the confidentiality, integrity, and availability of computing resources will be ensured. This will allow the hospital to function normally as a business and serve patients effectively and with privacy.

XI. Acknowledgements

A special thanks for Dr. G. K. IYER, He has provided valuable input and direction, and has supported me throughout this entire process. He has shown great patience while waiting for me to write, change direction, rewrite, slightly change direction, continue to write, and finish this research. Thanks to my parents for their unwavering love and support.

References Références Referencias

1. Affinity Press Release. url: https : / / www . affinityplan . org /uploadedFiles / Affinity _ Home / Who _ We _ Are / PressRelease _040510.pdf.
2. Carol Ag_ocs. \Institutionalized Resistance to Organizational Change: Denial, Inaction and Repression". In: Journal of Business Ethics 16 (1997), pp. 917-931.
3. Nessus Website. url: http://www.nessus.org.
4. ntop. url: http://www.ntop.org/.
5. OSSEC. url: http://www.ossec.net/.
6. Jeffrey Wheatman, Rob McMillan, and Andrew Walls. \How to Build a Computer Security Incident Response Team". In: Gartner Research Group (June 2010).
7. Microsoft Exploitability Index. url: http://technet. microsoft.com/en-us/security /cc998259.aspx.