Global Information Assurance Certification Paper

Securing the Employees in a HIPAA-Regulated Environment

Brian LaPointe
February 13, 2004
GSEC Practical Assignment
Version 1.4b Option 1

Abstract:

In the chain of corporate security, employees are often recognized as the weakest link. Firewalls, virus scanners, and security policies are often not enough to stop an employee from compromising the network and its data. An accidental click-and-drag of the mouse, answering "Yes" to pop-up dialog boxes, or a sticky note affixed to the side of the monitor are a few examples of how an employee can unknowingly compromise the network. In the majority of cases, the employee does not realize any harm has been done. The Health Insurance Portability and Accountability Act (HIPAA) further complicates the issues of corporate security for many companies. HIPAA creates national standards to protect individuals' medical records and other personal health information. This paper will explore the risks and the ways to mitigate those risks introduced into a HIPAA-regulated environment by the company's accidental attacker -- the employee.

Introduction

The Health Insurance Portability and Accountability Act, or HIPAA, is currently an item of major concern for many healthcare-related entities. According to Software Shelf International, Inc., HIPAA is "a federal law requiring hospitals, physicians, and managed care companies to adopt medical information security, privacy and data standards"[1].

In planning the security of an organization, it is easy to focus on outside threats such as the unknown hacker-for-hire motivated by money from a business competitor, or the bored teenager running widely available malicious scripts against your web servers. To consider these threats is, without a doubt, good practice. However, focusing on external threats alone and neglecting those that come from within can be a serious oversight.

This paper will cover several key areas of risk associated with employees, the relevance of the risks to HIPAA, and finally ways to mitigate them.

Scope

The HIPAA regulations impact a wide variety of computer operating systems from different vendors and between operating system versions. For the purposes of this paper, the focus will be on the current Windows environment (Windows 2000/2003 Server, and Windows 2K/XP workstation software).

Awareness

The most effective overall defense measure that can be implemented inside an organization is awareness. Employees should be the front line of internal defense, just as a firewall or edge router is for external defenses. An employee who knows what a virus is, and how it works, is less likely to open the important_memo.doc.exe attachment than an uneducated one. Which type of employee do you want in your organization? More importantly, which type do you have now?

To answer this question you will need to assess your employees' awareness. This can be a daunting task. You will need resources in the form of money for the services of a consulting firm, or just the time to develop the assessment yourself in-house. In order to get either resource, you will need support from the executive staff. Make sure the executives understand why you need a training program, the risks that drive it, and what can happen to revenues and company assets when employees are not security-aware. With proper executive backing, your plan will be more likely to succeed. Not only will you get the resources you need, but it will help to have the directors on board if when the employees ask, "Why do we need to take this ridiculous assessment? I've got better things to do!"

With executive support obtained, it is time to develop a user quiz. The quiz questions should pose real-world scenarios applicable to your computing environment. It should also present the employee with plausible multiple choices. The quiz answers should provide you with an understanding of the areas of security your employees are knowledgeable in, and those areas in which they are deficient.

After the assessment is complete, the next step is to develop a training program. This is your chance to address the areas which pose the biggest threats to your environment. Spending half of the training time focusing on laptop security when only 10% of your employees have laptops would be a waste of time. Spending time on areas in which your employees consistently scored well would be a waste of time as well. Remember that when you talk technical to end-users, they will tune out the conversation. Even if you do not develop or conduct the training in-house, you should at least select the areas you need to focus mainly on. Work out training goals based on those areas.

One common area that should be included in all security awareness training programs is Social Engineering. According to Dalton Design & Development Group, Social Engineering is "To use lies, deceit, play-acting and verbal cleverness to trick legitimate users into divulging the secrets of the system."[2] Because social engineering often forces employees to think on their feet, it is important that your training exposes them to the common techniques.

Keep in mind that over time, new threats will appear, and many of the existing employees will forget at least some of what you've taught them. A periodic refresher course and a follow-up quiz is just the thing to keep their awareness sharp and up-to-date.

Assessment

It is difficult to objectively assess the risks and threats to your network. Likewise, applying the HIPAA requirements to your specific environment can be confusing. An audit performed by a qualified firm can deliver a baseline assessment of your environment. External auditors are less likely to take business processes and statements for granted. As a result, they will expose shortcomings in your network's configuration that might otherwise be overlooked, saving time and money in the long run. Ernst & Young (www.ey.com) is one company that offers HIPAA compliance auditing services.

Covered Entities and Compliance

While the HIPAA regulations are focused on healthcare organizations, there are also provisions to address the organization's business associates. For example, if a patient's social security number appears on their health plan's member identification card, and the card itself is printed by a company other than the health plan, there are HIPAA implications. First, if the data is transmitted to the printing company across a public network, it must be encrypted. Second, the company printing the cards is also affected by HIPAA according to section § 160.103 of the Final Privacy Rule[3]. According to the American College Health Association, the covered entity (the health plan in this example) is "not required to monitor the activities of their business associates but would be required to take steps to address problems of which they become aware."[4]

There is no single HIPAA compliance strategy. Technologies and business processes vary from one organization to another. The HIPAA regulations were written to account for this by providing a degree of flexibility. Each identified action item in HIPAA is given a classification of "Addressable" or "Required." Items such as unique user names, or information system auditing are required. On the other hand, policies to automatically log off a user or verify the integrity of a transmission are addressable. While every company must be able to uniquely identify each user, automatically logging off the user after a certain time is not appropriate for all companies.

Penalties

The HIPAA legislation is meant to protect confidential patient information, or "Protected Health Information" (PHI). PHI is defined by the Partners Human Research Committee as "Individually identifiable health information transmitted or maintained in any form."[5] The violation of HIPAA standards leads to stiff penalties as described below by 45 CFR Parts 160 and 162:

> Section 1177 of the Act established penalties for any person that knowingly misuses a unique health identifier, or obtains or discloses individually identifiable health information in violation of this part. The penalties include: (1) A fine of not more than $50,000 and/or imprisonment of not more than 1 year; (2) if the offense is "under false pretenses," a fine of not more than $100,000 and/or imprisonment of not more than 5 years; and (3) if the offense is with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of not more than $250,000 and/or imprisonment of not more than 10 years.[6]

Problem Areas, HIPAA Relevance, Associated Risks and Mitigation

This section will outline in more detail, the areas of exposure employees are vulnerable to in their environment. First on the list and most prevalent – access to the internet through web browsing. Second is email, followed by network security. The remaining three risk areas are closely related – physical security (i.e. facilities), workstation security, and finally physical media.

Web Access

According to a survey conducted by the Internet Systems Consortium, the number of hosts on the internet more than doubled between January, 2000 and January, 2003.[7] The act of web surfing has become increasingly dangerous throughout the life of the internet. There are malicious sites lurking on the internet, waiting for an unaware user to visit. Some will take advantage of unpatched web browser vulnerabilities, thereby exposing the system to a slew of possible actions. Others will try to coax the user to supply private information, posing as a trusted site or authority. All of them have the potential to create serious security threats for your network.

Unfortunately, malicious web sites are not the only thing to look out for. Another risk associated with web access is malicious software. Malicious software can be broken down into three categories – adware, spyware and malware.

According to TechTarget.com:

> Adware is any software application in which advertising banners are displayed while the program is running[8].
>
> Spyware is any technology that aids in gathering information about a person or organization without their knowledge. On the Internet, spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties."[9]
>
> Malware (for "malicious software") is programming or files that are developed for the purpose of doing harm. Thus, malware includes computer viruses, worms, and Trojan horses.[10]

The difference between these three categories is primarily the software's intent. Whether the intent is displaying targeted advertising information, stealing confidential information, or inflicting harm to your computer system or data, there are risks involved for your network.

One example of adware is WeatherCast. According to Kephyr.com, WeatherCast displays the current weather conditions.[11] The weather is

something employees often want to know about to prepare for the ride home. To your employees, the WeatherCast software seems to provide a valid service. However, it also serves another purpose. Lurking within the installation package for WeatherCast is additional software called SaveNow. According to Doxdesk.com, "SaveNow is a single process run at startup which monitors open IE windows and opens adverts when it sees targeted URLs and terms entered into forms"[12]. Not only does it harvest information from the contents of the computer, but it also gleans information from the user's browsing habits in real time in order to display advertisements. As if this was not enough harm, TechTarget also states that "The WUInst variant can be used by any web site to download and install SaveNow or other code**."**[8] Any program that can download code from the internet without authorization is obviously a serious security problem. WeatherCast is but one of the countless adware-carrying software packages on the internet.

The risk presented by these malicious sites and software packages is enough to attract the attention of the HIPAA legislation. Section 164.308(a)(5) of the HIPAA security standards declares that entities should address user training for "Protection from Malicious Software"[13].

It is acknowledged as a problem by HIPAA. How can you help protect against web-based threats? The most obvious answer would be to completely restrict web access. This approach, however effective, would probably not be too popular. However, since popularity should not be the concern of a security administrator, it is still an option.

A more realistic solution would be a compromise that allows employees to browse the web, yet keep security in the picture. One such solution is a type of software known as a web filter. SurfControl Web Filter, by SurfControl, is one of the leading web filter packages.

A web filter is designed to monitor web browsing traffic from your employees to the internet, and then monitor the inbound response back to your employees from the internet. The technology works like a packet sniffer tailored for web traffic. It decodes the packets as they go to and from the user's computer, and determines the destination site the user is trying to access. From this point, it allows or denies access to the site based on how you have configured the software.

The filter itself should be positioned at a point in the network where it can "see" all outgoing traffic. In a network with a proxy server for web access, the filter is usually set to monitor the switch port used by the proxy server (in a Cisco switch, this is generally accomplished using the "set span" command). In a network using NAT (Network Address Translation), it would be placed at the limits of the internal network, on the inside interface of the firewall. Since there are many configuration options depending on the type of network, be sure to read the

corresponding documentation before deploying a web filter. See Figure 1 for a sample deployment location.

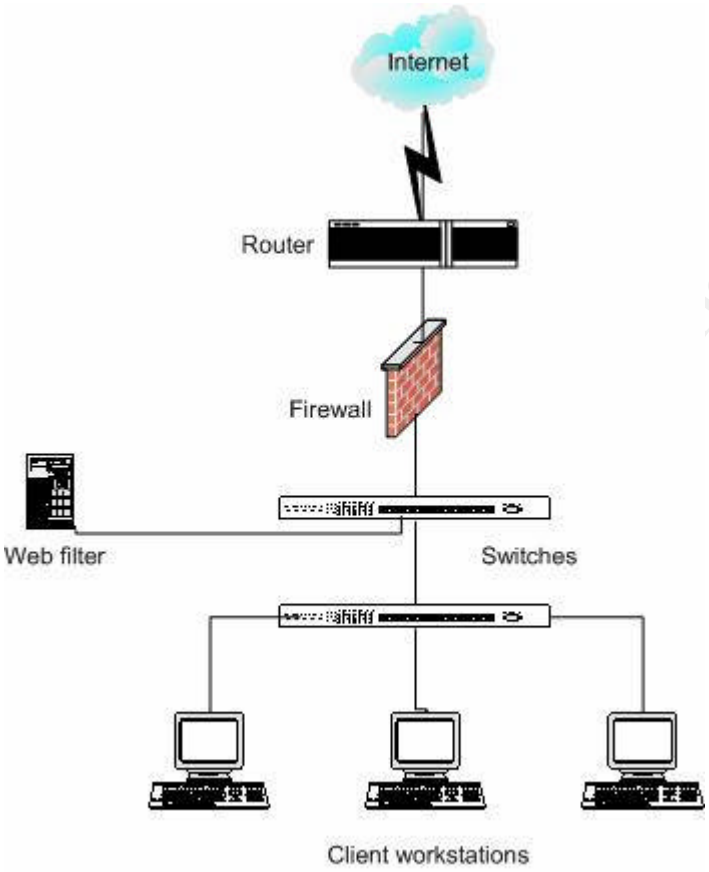

Figure 1
Suggested web filter deployment location

SurfControl Web Filter can control access to specific web sites – by category, name, and even by downloads. How many adware programs can an employee download if you deny access to .exe files? One of the most attractive features of SurfControl is that wider access can be granted to more security-conscious employees, while business-need only access can be given to regular employees. This flexibility lets SurfControl accommodate the various different types of employees in your organization. Another key feature is that Surfcontrol, as a company, has staff members working to categorize new web sites as they appear. This means that the product can address new threats as they are discovered on the internet.

Email

Within the last decade, email has gone from being a sparsely used technology to an indispensable method of communication in the corporate world. Email is constantly used by employees to communicate with contacts outside their company's network. Employees may not realize it, but there are definite security risks with email.

One risk involved in sending email over the internet is the exposure of confidential information both patient and corporate-related. HIPAA regulations mandate that PHI cannot be sent through conventional email unencrypted. There are several ways to achieve compliance with this regulation – training, email filtering, and secure messaging are a few.

Training

The training approach is very cost-effective. Your employees need to be aware that HIPAA regulations impact the ways they communicate with business contacts. They should be shown what constitutes PHI, and how to work around sending this information in email. Employees should also be shown how to deal with external contacts that send PHI into your company. The other companies your organization deals with on a daily basis will be at various stages of HIPAA compliance. It is in your best interest to let the sender know that emailing PHI is a serious problem.

Email Filtering

Email filtering software was originally designed to combat spam. Thousands of unsolicited emails are flowing into your network daily. Through the use of known spam tactics, filtering software can greatly decrease the flow of spam into your mail servers. Decreasing spam is not the only use of filtering software, however. For security purposes, two very important features make filtering a must. These are content filtering, and worm/virus protection.

Content filtering is the process of scanning email, as it flows in and out of your company's network, for specific patterns or properties. For example, consider the pattern ###-##-####. If an email goes out of the company with numbers matching this pattern, they almost certainly represent a social security number, which is PHI. With content filtering, you can scan all email for this pattern and prevent it from entering a public network. If the email was inbound, you can send an email to the sender and inform them of the problem. Content filtering can also scan for indicators of proprietary company information, or other sensitive information that should not leave the company.

While content filtering helps an organization maintain HIPAA compliance, an email filter can also help protect against email-borne worms and viruses.

Scanning for dangerous attachments (.exe, .com, .bat, .vbs to name a few) and stopping them from entering the network can be an invaluable security measure. Antivirus software positioned to scan all inbound mail is a good security measure. However, new worms and viruses are created every day. At the first launch of an email-borne virus, antivirus definition files usually aren't equipped to detect the worm. An email filter configured to scan for potentially dangerous attachments entering the company will stop the new virus before it can infect your systems.

Some special exceptions may need to be made depending on your organization. For example, a contact that is not yet equipped with the proper encryption or FTP capabilities may send a self-extracting, password protected file via email. While this is not desirable and probably not HIPAA compliant, it could still be necessary for your company to continue daily business. If you must make exceptions for dangerous incoming attachments, do it on a per-sender basis. Don't allow all executables from an entire domain just because one contact there needs to send .exe attachments.

Secure Messaging

Conventional email is not secure. Email sent through a server without encryption or similar security precautions is sent in clear text, and easily intercepted. When PHI must be transmitted across a public network, encryption is a necessity. The most popular email server suites (Microsoft Exchange, Lotus Notes, for example) offer secure communications options, but this can be a burden to set up and maintain. There are alternatives which may be simpler to set up and manage.

One alternative is to use a web-based email solution. This allows web access, through SSL (Secure Socket Layer) encryption, to an online email account. This solution provides an encrypted medium for email that presents only a small change to the user (the fact that it is web-based). This option can either be implemented in house, or through a third party.

Another growing trend is to use a network appliance such as Neoteris IVE (http://www.neoteris.com/products/functoverview.html) to provide external contacts access to network resources. This solution, similar to the above web-based email solution, uses SSL encryption to secure the connection. However, Neoteris IVE is a much more robust solution. It can be configured to provide authentication by multiple methods (native users, RADIUS, RSA SecurID, etc). Also, one particularly useful feature of Neoteris IVE to a HIPAA-regulated organization is the ability to grant an external contact access to internal network shares. With this configuration, the external contact can upload (or download) data securely to a location that your employees can access from their desktop without any additional configuration. The convenience for your employees and their contacts is unmatched by other email solutions, and the data is securely transmitted.

Remember to implement layers of defense. An email filter can stop potentially dangerous attachments, but exceptions can be made. An up to date antivirus server, configured to scan all inbound messages that make it past the filter, is a second layer of defense. The third layer is antivirus software on the desktop. Finally, increase your employee awareness regarding the dangers of email (and the impact of HIPAA). The combination of these four measures greatly increases your protection.

Network Security

So far this paper has covered how an employee can inadvertently introduce vulnerabilities into the network via web access or send and receive information restricted by HIPAA via email. This section focuses on the threats posed to the network by the employees themselves.

According to Gartner, Inc., "more than 70% of unauthorized access to information systems is committed by employees"[14]. However, the majority of those employees are not hackers. They are not intentionally trying to find ways to compromise the security of your servers, nor are they trying to expose PHI to unauthorized personnel. That is the good news. The bad news is that they are doing all of this *without* trying.

The failure to properly secure network shares is the principal cause of confidentiality infringements within an organization. A share is a network resource that users have been granted access to use remotely. By default, all users in a domain are granted access to the share. Shares come in many flavors, such as the employees' personal drives, public file server drives, and departmental drives. In terms of security, each of these has different implications.

Personal shares possess the least risk. Their general purpose is to give an employee a network-based location to save data. Normally, only the user and necessary systems-administration personnel should have access to this type share.

Public shares are more of a risk than personal shares. They generally allow open access to many users. This is where permissions and training come into play. For a public drive that is meant to be fully accessible for all employees, training is the key. Users need to be able to recognize PHI (or other sensitive information), and know how to apply permissions to their own folders and files. A public shared drive should not be seen as a dumping ground for anything anyone in the company might need to access. Your employees should see it as a means of sharing information within the company in a secure manner. If your company does require the use of public drives, proper training is the sure way to keep them secure.

Departmental shares are an easier risk to manage. These are designed to provide a common location for one department or business unit to share documents with its own staff. Departmental shares limit data access to functionally similar personnel. Since departments are usually predefined groups in the corporate structure, configuring shares for each department should be a simple task.

In order to facilitate security permissions for shares, the organization needs to be broken up into groups. Adding the 30 members of the finance department to the access control list (ACL) for the finance departmental share would not only be tedious, but difficult to manage. Similarly, trying to pick out the handful of employees that need access to data files containing PHI is inefficient.

Instead, a better choice is to put the users into logical groups and organizational units. The best strategy to accomplish this in a HIPAA environment is to use role-based security. The idea behind role-based security is very similar to an important security concept – the principle of least privilege. Rather than grouping users solely based on their departmental affiliation, they are grouped based on their functional responsibilities.

Consider a claims department of 5 people. Of these 5 people, there is a manager, an administrative assistant, and three claims processors. All 5 employees are in the claims department. Does that mean they all need access to the same data? The three claims processors do not need access to budgeting data, but the manager does (and perhaps the assistant as well). The administrative assistant does not need access to anything related to patient claims, but the manager and the claims processors do. By grouping users based on their role, permissions to sensitive information on the network can be set more specifically. The resulting roles for this example might be named “Claims Manager”, “Support”, and “Claims processor”. Permissions to network resources could then be allowed or denied based on what each role needs to do their job.

One added benefit of role-based security is the ability to facilitate employee position changes. When a claims processor accepts a new position of sales manager, she no longer needs access to the same type of data. Instead of digging through the network to find all the resources where the user’s name is on the ACL, the administrator can simply remove the “Claims processor” role and add the “Sales Manager” role.

When properly planned and implemented, role-based security is a very effective way to maintain appropriate levels of access for each member of the organization.

Physical Security

An employee in your mailroom needs to go out to the dumpster to dispose of some cardboard boxes. So, he heads for the back door near the loading dock with boxes in hand. It is a short trip to the dumpsters from the loading dock, but it's cold out there this winter. His company-issued ID badge does not allow him access into the building through the back door – it would lock him out if he let it close, forcing him to walk all the way to the front of the building. So, he just props some cardboard in the doorway to stop the door from locking behind him. After all, it is just the back door. What is all the fuss about?

As a security professional, this scenario should make you cringe. Permission lists and firewalls do not protect your data from someone who is physically in your company's building. The intruder, waiting for an opportunity such as the one presented above, strolls through the back door into your mailroom. From here, where does he go? Is your data center door secured? Will someone know to stop him? Or will they just smile and wish him a nice day as he carries a desktop back out to his car…

The physical security of the building is an important aspect of the overall security of your data. To achieve acceptable physical security, you will need technical measures, and employee training.

The most common technical measures include ID badges, smart cards, biometric devices, and monitoring devices. An ID badge of some sort is a must for any organization. You need to be able to identify that a person is an employee, and an ID badge with a photo is ideal.

ID badges can also be enhanced to function as smart cards. This combination gives multiple layers of access control. Not only must the photo on the badge match the person presenting the badge, but the employee's name (or other identifying information such as employee number) embedded in the smart card must also match the access list for the building/door the person is trying to enter.

Biometric devices, such as fingerprint readers or retinal scanners, greatly increase security. Modifying a badge to have an intruder's picture on the front instead of the actual employee is not difficult. But the intruder's chances of modifying her fingerprint to match that of the actual employee are not high.

Once the physical identification and authentication methods are in place for your building, it is still important to be able to monitor key areas remotely. Placement of cameras (or other physical monitoring devices) in key areas will maximize the reach of your facility's security personnel. A camera pointed at the back door in the mailroom example above would have alerted your security guard to see that an outside door has been propped open, allowing him to react. A sensor on the

lock indicating the door has remained open for more than 10 seconds could also tip off the guard.

The above technical measures, and an alert security guard, can greatly increase the overall security of the building. However, physical security should be the responsibility (and concern) of every employee. Once again, an employee training initiative is necessary for this to happen. First, employees should be encouraged to challenge any person not wearing identification. If someone is not wearing their badge, or looks unfamiliar, your employees should not hesitate to stop them. Second, employees need to be educated on why building doors should be secured. To some, the locks on outside doors are nothing but a nuisance. Make sure they know why it is in their best interest to keep locked doors locked. Finally, teach the employees that it is OK to report suspicious activity to the security guard, or their supervisor.

Workstation Security

Returning to the example of the propped-open back door discussed previously, the intruder that managed to sneak into the building is wandering around your building. He can't actually log into the network, right? After all, your network logons are required to use strong passwords. Always one to follow best practices, you require the user to choose a password that is at least 8 characters in length, uses both uppercase and lowercase letters, with at least one number and symbol. The password changes every 60 days, and the user is not allowed to reuse the 10 most recent passwords. This strategy indeed results in requiring users to select strong passwords. Unfortunately, it sometimes also results in the user's inability to remember their password. Enter the sticky note.

There is nothing worse than stopping to work on an employee's computer, and seeing a yellow sticky note on the monitor with "J$mith01" written on it. You will not need long to guess what that note is for. Neither will the intruder wandering through your building. The password may meet the complexity requirements of the security policy, but is no longer secret.

Another workstation security risk is remote access. Whether it is an employee in the finance department that needs to transmit data to a bank using a modem, or a telecommuter with a remote-control software installed on his PC at work, the risk to your network is high.

In both cases, a back door is introduced to the network by the employee. Any device which bypasses the external access controls, and allows access into the network is a serious risk. What good is your firewall, if the attacker can dial directly into an internal workstation?

To minimize the number of attack entry points in your network, eliminate all unnecessary remote access devices/programs. For those that can not be eliminated, ensure they are configured correctly. In the case of modems, one option is to set the call-back option. An attacker is not going to accept a return call from the modem he is trying to connect to. For remote-control software, make sure a password is required, and changed regularly. Systems providing remote access should be configured to keep detailed logs of connection attempts, both successful and failed.

Apart from mitigating the workstation risks outlined above, it is important to create (and enforce) an appropriate workstation security policy. For example, make sure the policy includes provisions to either bring up a password-protected screen saver or log off the user after a period of inactivity. A complex password does no good if the workstation remains active and unlocked when a user leaves his desk.

Physical Media

In order to protect against the threats of malicious software as described earlier, you have implemented a web filter which prevent users from visiting known adware sites. So your employees can't get adware programs on their PCs, right? You have also implemented an email filter to stop email including sensitive information (such as PHI) from exiting the company unencrypted. So you have stopped users from placing member information in unauthorized hands, right? Unfortunately, the answer to both of these questions is no if you have not considered removable media and portable computing devices.

Removable media, such as floppy disks, recordable CDROMs, and USB storage devices, present a difficult risk to manage. Because of their limited storage capacity, and the fact that they are slowly being phased out of production, the risk posed by floppy disks is less significant. Recordable CDROMs and USB storage devices, however, are widely available.

Recordable CDROMs (and more recently, DVDs) give the user the ability to store large amounts of information on fairly cheap media. If an employee has a relatively new computer at home, it is likely that some type of recordable CDROM or DVD drive came with it. The earlier example of using a web filter to stop employees from getting adware programs on their PC is easily circumvented by removable media. All the employee needs to do is download the program they want from their home PC, and burn it to a CD. When they return to work the next day and pop the CD in, your web filter provides little protection against this threat.

To counter this problem, a policy can be created that prevents the installation of a program from removable media. This can easily be done using the Group Policy Object feature in a Windows 2000/2003 Server environment. In Windows XP, the policy is located in User Configuration -> Administrative Templates -> Windows Components -> Windows Installer, "Prevent removable media source for any install".

Besides bringing data into the company, removable media can be used to bring valuable or confidential data out. The storage capacity available in the newest removable media devices (specifically DVD-R, and USB) has increased over the comparatively smaller CD-R specifications. When combined with the small size and inconspicuous appearance, these devices present a greater security risk.

Conclusion

The protection of PHI is the main goal of the HIPAA standards. Since it is the employees that handle PHI on a daily basis, a successful HIPAA compliance strategy is one centered on the employees. Start with a comprehensive security training and awareness program. Once the employees are aware of the risks and well educated against them, implement the appropriate technical measures in conjunction with a well-planned and enforced corporate security policy. If done well, you will confidently diminish the risks introduced by employees.

Although HIPAA compliance is an attainable goal, your responsibility to protect the network and prevent PHI exposure does not end with just formal compliance. Your company policies and procedures are dynamic and will change often. To keep up with those changes, perform annual internal audits along with using outside auditors every few years to insure continued compliance. Without the annual audits the possibility of new risk exposures increases. Those new risks must be addressed or be prepared to face the penalties.

References

[1] Software Shelf International, Inc. "IT Dictionary." URL: http://support.softwareshelf.com/dictionary/default.asp?l=h (2 Feb. 2004).
[2] Dalton Design & Development Group. "CyberCop – Security Resources: Glossary." URL: http://www.3dg.com/cybercop/resources/glossary.html (2 Feb. 2004).
[3] Department of Health and Human Services, Office of the Secretary. "45 CFR Parts 160 through 164." Standards for Privacy of Individually Identifiable Health Information. 28 December 2000. URL: http://aspe.hhs.gov/admnsimp/final/PvcPre01.htm (6 Feb. 2004).
[4] American College Health Association. "HIPAA Definitions." URL: http://www.acha.org/info_resources/UF_HIPAA_Definitions.pdf (6 Feb. 2004).
[5] Partners Human Research Committee. "HIPAA GLOSSARY." Partners Human Research Committee Policies and Procedures. 28 October 2002. URL: http://healthcare.partners.org/phsirb/hipaaglos.htm (5 Feb 2004).
[6] Department of Health and Human Services, Office of the Secretary. "45 CFR Parts 160 and 162." Health Insurance Reform: Standards for Electronic Transactions. 17 August 2000. URL: http://www.cms.hhs.gov/hipaa/hipaa2/regulations/transactions/finalrule/txFR.asp (6 Feb. 2004).
[7] Internet Systems Consortium, Inc. "Internet Domain Survey, Jan 2003." URL: http://www.isc.org/index.pl?/ops/ds/ (2 Feb. 2004).
[8] TechTarget. "adware – a whatis definition." URL: http://whatis.techtarget.com/definition/0,289893,sid9_gci521293,00.html (5 Feb. 2004).
[9] TechTarget. "spyware – a searchCRM definition." URL: http://searchcrm.techtarget.com/sDefinition/0,,sid11_gci214518,00.html (5 Feb. 2004).
[10] TechTarget. "malware – a searchSecurity definition." URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci762187,00.html (5 Feb. 2004).
[11] Kephyr.com. "WeatherCast – Adware removal instructions." URL: http://www.kephyr.com/spywarescanner/library/weathercast/index.phtml (5 Feb. 2004).
[12] Doxdesk.com. "and.doxdesk.com: parasite: SaveNow." URL: http://www.doxdesk.com/parasite/SaveNow.html (Feb. 5 2004).
[13] Department of Health and Human Services, Office of the Secretary. "25 CFR Parts 160, 162, and 164." Federal Register Part II Health Insurance Reform: Security Standards; Final Rule. 20 February 2003. URL: http://aspe.hhs.gov/admnsimp/FINAL/FR03-8334.pdf (5 Feb. 2004).
[14] Gartner, Inc. "Attackers Take Advantage of Employees." URL: http://security2.gartner.com/story.php.id.38.s.1.jsp (5 Feb. 2004).

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event