Are You Vulnerable to Hackers?

Save to myBoK

by Joseph L. Sardinas Jr., PhD, and Jeannine D. Muldoon, PhD, RN

You might think computer hackers' activities are restricted to viruses and hoaxes. Unfortunately, their repertoire is far larger, which puts your facility's computer system-and patient privacy-at risk. This article provides a look at how hackers work and the best ways to protect your systems.

More members of the healthcare community use the Internet every day. Web sites providing access to medical information, patient records, and other data can enhance healthcare providers' ability to care for their patients as well as facilitate their "virtual presence" to serve the needs of a faraway patient. Unfortunately, it can also allow unauthorized access to patient medical records, leading to privacy violations or destruction or modification of patient information. The convergence of unique technologies to assist patients along with cyber criminals demands that the healthcare profession carefully consider the risks inherent in this technology.

Hackers: Everywhere and Often Invisible

Becoming a target for hackers is as easy as connecting to the Internet. Often, the most basic security measures are not implemented. For example, nearly a third of e-businesses don't use a firewall (hardware or software that sits at the perimeter of a network and permits or denies access to a network), often considered the first level of defense and most common security precaution taken by organizations tied to the Internet.[1, 2] Unfortunately, many new Internet-based systems are quickly created and security is given minimal consideration, if at all.

According to a recent survey of US corporations, government agencies, financial institutions, medical institutions, and universities by the Computer Security Institute (CSI) in conjunction with the Federal Bureau of Investigation (FBI), 85 percent detected "cyber attacks."[3] Further, 186 organizations who were able or willing to quantify the financial impact of cyber intrusions reported more than $377 million in losses or an average loss of $2 million per organization. That compares with 249 organizations reporting more than $265 million in losses or an average loss of $1 million in 2000. The average loss has increased by approximately 90 percent in one year. Security breaches included theft of proprietary information, financial fraud, system penetration from outsiders, denial of service attacks, and sabotage of data or networks. Seventy percent of respondents cited their Internet connection as a frequent point of vulnerability. From physicians in private practice to major healthcare facilities and managed care organizations, the entire healthcare community is vulnerable to hackers or crackers (criminal hackers).

Hackers can inflict a variety of damage on the computer systems of medical facilities. In one "cyber attack," patients' cancer test results were changed from negative to positive and in another, surgery had to be postponed after an intruder accessed CAT-scan data.[4] A major medical center was the target of a cyber intrusion, and the hackers accessed thousands of medical records of heart patients. These records included patient names and Social Security numbers.[5] The fundamental problem, however, is that no more than 10 percent of all computer-related attacks are even detected.[6] This suggests that cyber intrusions are taking place in healthcare facilities right now, and the targeted facility doesn't even know it's being hacked. Security experts suggest that the majority of computer break-ins are not identified because:

- hackers have sophisticated methods
- the tools needed to determine the degree of intrusion are not available
- many managers still refuse to devote sufficient resources for basic risk management
- the FBI and other law enforcement organizations do not have adequate resources to train electronic experts[7]

What's in the Hacker's Arsenal?

There are many ways hackers can gain access to patient information. “Spoofing” is a method where the attacker runs a software tool that creates Internet messages that appear to come from a “trusted” computer and not the hacker’s computer. The “trusted computer” will be given access to the target computer. Consequently, the hacker can gain entrance to the target medical computer, and access, modify, or destroy the data. To accomplish the same objective, a hacker can use a “sniffer,” which monitors traffic on a network, including the Internet. The sniffer permits the hacker to capture every packet of data on the network and read the contents.[8] A hacker can use the sniffer to capture account numbers and passwords to the medical information system, then log on and access the data. Hackers can also write a virus to destroy all data and send an e-mail with the virus as an attachment.

Keep in mind that a hacker need not be a technological whiz. Highly sophisticated hackers often identify a weakness in an operating system or application program and write programs to exploit it. Hackers often post these programs on selected Web sites where they can be downloaded even by kids-these programs are often called “kiddie scripts.” As a result, anyone who knows how to download a file from the Internet and then run it can become a hacker.

Even the best-protected computer systems are still vulnerable to a denial of service attack. In its simplest form, a denial of service attack (also called SYN [synchronized] flooding) can render servers inoperable. A small utility can flood the target computer with half-open connection requests. That is, it sends a message to the target, and the target tries to respond, but can’t find the recipient. It waits for a period of time (say 50 seconds), and then times out. If hundreds of these messages are sent every second, the target computer becomes overloaded. With a distributed denial of service attack, the perpetrator takes over several computers, referred to as “zombies,” and each one of them sends messages to the target computer. In both cases, no data is accessed or destroyed-the computer simply crashes.[9] If a healthcare provider is attempting to access a patients’ medical records, or some form of telemedicine is in operation, both activities will be halted and the patient potentially placed at risk.

Not Idle Threats

The Center for Strategic and International Studies (CSIS) is a public policy research institution that maintains experts on key functional areas such as national and international security issues, energy, telecommunications, and trade and economic policy.[10] CSIS identified four general threats that computer-based systems may face in the 21st century:[11]

- **Disruption**: Communication, economic transactions, electrical power grids, water distribution, and other components of the national infrastructure may be compromised. From a healthcare facility perspective, disruption may be the result of a hacker accessing the operation of the facility’s computer system. If a medical facility’s computer system is brought down, the implications to patients may be critical.
- **Exploitation**: Unauthorized access to and use of sensitive, proprietary, or classified information will have a serious effect on the targeted medical facility. From a healthcare facility perspective, this threat directly relates to the new privacy protection regulations under HIPAA.
- **Manipulation**: Modification of patient medical records for political, economic, or other personal gain can trigger life-threatening situations. Consider the example above where patients’ cancer test results were changed from negative to positive. This event would clearly fall under the HIPAA privacy rule.
- **Destruction**: To cause patient medical records to be destroyed in whole or in part also falls within the HIPAA regulations. Destruction of information is of particular concern because it can be done quite simply, and if proper back-up procedures have not been initiated, the records may be unrecoverable.

It is important to note that the above threats may be perpetrated by individuals who reside in a different city, a different state, or a different country. Moreover, a hacker may take control of a computer in an entirely different country, and launch the “cyber attack” from that computer, making it more difficult to trace the hack. In addition, if the intermediate computer usurped is powerful, the damage done to the target facility may be substantial. It must also be remembered that the perpetrator may be inside your facility.

What’s the Motive?

Why do hackers hack? The following may provide some insight:[12]

- **Spite**: The hacker may simply dislike your organization. An individual may feel "wronged" in some way, whether actually or philosophically. It is a form of revenge.
- **Sport**: Perhaps you have a brand-new system that has just come online with great fanfare in the press. It's a tempting target.
- **Profit**: The hacker may try to steal patient information for "blackmail" purposes or has been paid to retrieve information, destroy data, or interrupt operation of your computing facilities.
- **Stupidity**: Many crackers attempt to impress others by performing acts that cause problems.
- **Curiosity**: Many hack into systems just to see if they can do it. They derive enjoyment from the process.
- **Politics**: Some are "hactivists" who have a political agenda. They seek coverage in the media to highlight a particular cause. Your medical facility may be performing procedures they oppose or not performing procedures they support.

Whatever the reason, hackers can cause substantial damage to a healthcare facility's computer system. Moreover, if patients' medical records are not protected, according to the new regulations, there may be civil and criminal penalties. These penalties, it is presumed, will spur medical facilities to institute appropriate policies and procedures to minimize the risk of patient medical record compromise.

A System of Security

How should the privacy officer protect patients' medical records in an electronic environment? One might think that the person responsible should generate a list of all the latest security hardware and software and begin buying and implementing it. However, this approach will lead to uncoordinated attempts to secure the system. The privacy officer must understand that security is an ongoing process. It's dynamic and must continuously evolve and adapt as technology and hacker sophistication increase. Procedures must be in place to insure that the latest fixes from software vendors are applied to the operating system and application programs. Further, continuous training of key systems personnel is essential. Finally, the privacy officer must think like a hacker, including visiting Web sites that hackers use to locate the latest vulnerabilities in software.

All too often, we look for a "silver bullet" solution. Unfortunately, one does not exist. A logical approach to the development of a system of security must be employed (see "A Systems Approach to E-mail Security"). Further, risk assessment is crucial to the entire process. The risk assessment will evaluate threats and attempt to quantify potential losses. Performing calculations to help understand and manage risk is an important component.

The primary goal of privacy personnel is to protect the privacy of patients' medical records. Other considerations, such as making sure telemedicine capabilities are not hampered and that computer systems remain stable, up, and running are also important goals. A systematic approach using a well-established problem-solving methodology will help the healthcare community meet the privacy needs of patients.

A Systems Approach to E-mail Security

General systems theory provides a unified method for solving problems. For our purposes, the word "system" will mean a set of elements that are interrelated and interact toward one or more common goals or objectives.[13]

Attach Costs to Risks

Risk management is an important component when considering the process of security.[14] This is true when we decide whether to put a lock on the front door of our home or the privacy officer of a healthcare facility decides whether to implement a firewall.

According to James DeLoach, a risk management consultant, "Risk management must be integrated with business planning and strategic management so that it becomes inextricably linked to those processes."[15] The goals, objectives, and policies of risk management must be clearly stated and communicated throughout the healthcare facility and aligned with overall business objectives, strategies, and performance goals. Risk of unauthorized access must be balanced against the need to ensure that information can be retrieved easily when required for care.[16]

Equally important, cost must be associated with risk. How much does a door lock cost versus the potential loss if thieves entered your home and carried away everything they could? If an unauthorized user could access a healthcare facility's computer system and cause $250,000 worth of damage, is it worth spending at least some portion of that potential $250,000 loss on a firewall and other security measures to safeguard patients' medical records?

We often talk about taking a "calculated risk," yet how often is anything actually calculated? It is important to note that no matter how much money one spends, absolute security is not attainable. What we must determine is a level of risk that is acceptable. By imposing civil and criminal penalties for not securing patient medical records under HIPAA, the Department of Health and Human Services is attempting to persuade administrators to make security part of the strategic business plan and to spend the necessary money to implement the security measures.

In the light of general systems theory and risk management, the "systems development methodology" may be employed. The systems methodology to solving problems is comprised of seven stages: definition, analysis, planning, design, implementation, evaluation, and maintenance. The seven stages may be applied to each of the stages individually where appropriate.

Setting Goals, Performing Analyses, Making Plans

The following is an example of how the systems approach methodology may be applied. Let us assume that the **goal** for our example is to use an e-mail system to send patient medical records to another healthcare professional while assuring patient medical record privacy.

Our **analysis** determines what e-mail is, how it works, and its benefits and risks. E-mail is an electronic method of transmitting information via a network to other individuals. The network may be local, wide area, or the Internet. Most e-mail systems are comprised of two parts: a user agent that permits a user to create, edit, store, and forward e-mail messages and the message transfer agent, which prepares and transfers the e-mail message. Once the e-mail and any attachments have been created, the Internet protocol Simple Mail Transfer Protocol (SMTP) is used to perform the transfer.[17] Information moves across the Internet as data packets, also known as datagrams. Data packets are like large envelopes that contain whatever information is being transferred along with all required header (or addressing) information. In the case of e-mail, one might imagine that the e-mail message is placed within the data packet "envelope" as it moves through the network looking for the proper address to deliver the message.

As it moves along the network, the message actually encounters many computers. At each one, the computer looks at the header information and says, "It's not for me," and the message keeps moving. At the receiving end, an e-mail daemon (a program running in the background) watches port 25 for any incoming messages. Port 25 is generally reserved specifically for e-mail. If the receiving computer is turned off, the Internet service provider's (ISP) server saves the e-mail using Version 3 of the Post Office Protocol (POP3) until the receiving computer is once again online and the user can download the message from the server.

As we perform the analysis, we realize that sending e-mail can lead to a variety of results. First, it may be sent to the correct individual and properly read. Clearly, this is the desired outcome. However, there is potential for other problems. E-mail may be sent to the wrong individual, because of an incorrect e-mail address, a typographical error when entering the e-mail address, or an error in the system. Or e-mail may be read by an unauthorized individual at a valid e-mail address location. For example, an unauthorized individual may be sitting at the receiving computer and could simply open the message.

In addition, information systems personnel in charge of the network servers at the receiving or sending healthcare facility may "trap" the e-mail and read it. Or e-mail may be intercepted, read, or modified by an unauthorized individual outside either the sending or receiving healthcare facility using a sniffer.

If the information in the e-mail contains patient medical records in plain text, then that unauthorized individual can read the records.

When performing an analysis, we must think beyond the obvious. Specifically, when evaluating the use of e-mail, we must not only consider the fact that the e-mail message itself may be compromised, but the e-mail system on your facility's computers may be the target of unauthorized access and therefore just having an e-mail system can cause the entire computer system to be vulnerable to hackers. The computer system may be compromised in several ways, including but not limited to hacking into your computer system and gaining access to all patient medical records or exposure to e-mail viruses. Given the above analysis, alternative plans must be developed.

Plan 1

One possible plan is not to use e-mail, but instead use another form of communication. Other forms of communication may include telephone, fax, postal service, courier, etc. If this plan is selected, then each alternative method must itself be evaluated.

Plan 2

A second potential plan might be to establish a direct, dedicated, and secure line of communication with the other healthcare provider. This might increase the level of security, but the cost of such a connection might be prohibitive. Moreover, such a connection would be with only one other healthcare provider. This alternative will not handle the transmission of patient medical records to other healthcare providers. Therefore, if this plan is selected, it would be expensive and limited in use.

Plan 3

A third potential plan might be to evaluate the risks and determine if cost-effective controls can be identified to contain those risks. Based on the discussion above, four general weaknesses were identified. Each weakness must be evaluated and an appropriate control be identified.

To determine who actually sent the message, digital signatures are a valuable tool. Digital signatures use encryption to transform a message in plain text into an unreadable message.[18, 19] Essentially, the person sending the e-mail encrypts the message using a particular key. The receiver has a second key that decrypts the message. The second key will only decrypt a message encoded with the first key. Therefore, only the authorized sender could have sent the message if the second key decrypts it. Moreover, the encryption mechanism has a built-in facility that will determine if the message has been tampered with. Properly used digital signatures are recognized by the federal government, as well as the American Bar Association.[20]

Encryption can also protect against misdirected e-mails. If we assume that the method of encryption is strong, even if a message goes to the wrong individual, that person would not be able to decipher the message. Similarly, encryption can protect against unauthorized readers at a valid e-mail address location.

However, if decryption is automatic, then another control limiting access to that, or any other computer, should be used. Specifically, if the computer is left unattended for a very short period of time, it should automatically lock and prevent access unless a secure method of access is used. This may include a password, a biometric, or a card with a magnetic strip containing proper information. This would effectively prevent access to any portion of the system, and appropriate logging activities could provide documentation showing who accessed the machine, when it was accessed, what was accessed, and for how long.

If access to the computer is not limited, decryption should not be automatic: only the valid receiver of the e-mail should have a decryption key to read the e-mail instead of allowing the computer to automatically decrypt the message with a saved key. Thus, anyone not knowing the key could not read the e-mail. In either event, proper procedures will have to be established at the receiving site to ensure that neither decryption keys nor passwords are posted in plain sight nor access cards are shared or otherwise made available.

Encryption can also protect against the possibility that e-mail may be intercepted, read, or modified by an unauthorized individual outside either the sending or receiving healthcare facility. If the message is encrypted, it cannot be read by anyone not knowing the decryption key. If a digital signature is used, any attempted modification of the message would be detected.

Finally, we must evaluate risk that the computer system itself may be compromised through using an e-mail system. How can a healthcare facility minimize the probability that an unauthorized person will hack into a system? A firewall is often considered to be the first line of defense. Stronger controls might be required depending on the nature of the connection to the Internet. For example, if a computer uses a dial-up modem and is connected to the Internet for a very short time only to send and receive e-mail, a firewall might be sufficient. However, if the computer system is connected to the Internet 24 hours a day, seven days a week, additional controls may be necessary.

Other considerations might include whether the computer is a part of a larger network. Clearly, the more complex the system, the more complex will be the required security controls. Lastly, to protect against unwanted viruses, appropriate anti-virus software would need to be installed along with standard procedures regarding the handling of e-mails from unknown senders.

After evaluating each of the above plans and calculating costs, let's assume we select plan 3. There is a cost associated with encryption software, digital signature software, a firewall, anti-virus software and all procedures required, but it is determined that the benefits outweigh the cost and plan 3 is chosen.

From Design to Maintenance

Once the plan has been selected, the **design** phase is engaged. E-mail encryption software, digital signature software, firewalls, anti-virus software, and appropriate procedures are evaluated for strength of security, cost, and compatibility with existing hardware, software and current practices, procedures, and policies. The selected security controls are obtained and installed. They are fully tested with non-sensitive information.

When all tests are complete, **implementation** occurs. All e-mail containing patient information passes through the encryption software, digital signatures are utilized, the firewall is established and anti-virus software is activated. The security controls are **evaluated** in a production environment. Any weaknesses must be addressed immediately. The systems development methodology is also evaluated.

Finally, the security controls to protect e-mail and the computer system will be updated by the vendors. Maintenance of these controls is vital to the continued security of the e-mail system. Vendor updates will contain fixes to known problems as well as enhancements to the product. All updates should be installed immediately. **Maintenance** is an ongoing process-just like the process of security. All the above notwithstanding, the weakest link in the process of security may be the person receiving or sending the information: inappropriate conversations may undermine all of the above security controls.

Notes

1. Berinato, Scott and Renee Boucher Ferguson. "Hack Alert: Where's the Outrage?" *eWeek*, September 18, 2000. Available online at www.eweek.com.

2. Bertin, Michael. “The New Security Threats: Target Practice.” *Smart Business*, January 16, 2001. Available online at www.zdnet.com/enterprise/stories/main/ 0,10228,2669953-2,00.html.

3. Computer Security Institute. “Computer Crime and Security Survey.” Available online at www.gocsi.com.

4. Machlis, Sharon. “Congressional Panel Hears Troubling News on Hackers.” *ComputerWorld*. March 13, 1997. Available online at www.computerworld.com/cwi/story/0,1199,NAV47_STO23470,00.html.

5. Berinato, Scott. “The Year of the Killer Hackers and Other Tales of Security Woes Facing IT.” *eWeek*, December 18, 2000. Available online at www.zdnet.com/eweek/stories/general/0,11011,2665640,00.html.

6. Borchgrave, Arnaud et al. “Cyber Threats and Information Security Meeting the 21st Century Challenge.” *Center for Strategic and International Studies*, December 2000. Available online at www.csis.org/homeland/reports/cyberthreatsandinfosec.pdf.

7. Ibid.

8. Anonymous. *Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network*. Indianapolis, IN: SAMS Publishing, 1998.

9. Schneier, Bruce. *Secrets & Lies: Digital Security in a Networked World*. New York: John Wiley & Sons, 2000.

10. “CSIS at a Glance.” Center for Strategic and International Studies. Available online at www.csis.org/about/.

11. “Cyber Threats and Information Security Meeting the 21st Century Challenge.”

12. *Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network*.

13. Sardinas, Joseph L. *Computing Today: An Introduction to Business Data Processing*. Upper Saddle River, NJ: Prentice-Hall, Inc., 1981.

14. *Secrets & Lies: Digital Security in a Networked World*.

15. DeLoach, James. *Enterprise-wide Risk Management: Strategies for Linking Risk and Opportunity*. Upper Saddle River, NJ: Financial Times Prentice Hall, 2000.

16. Committee on Maintaining Privacy and Security in Healthcare Applications of the National Information Infrastructure. *For the Record: Protecting Electronic Health Information*. Washington, DC: National Academy Press, 1997.

17. White, Curt M. *Data Communications and Computer Networks: A Business User's Approach*. Cambridge, MA: Course Technology Publishing Company, 2000.

18. Computer Security Division, Information Technology Laboratory. “Federal Agency Use of Public Key Technology for Digital Signatures and Authentication NIST Special Publication 800-25.” *National Institute of Standards and Technology*. October 2000. Available online at http://csrc.nist. gov/publications/nistpubs/800-25/sp800-25.pdf.

19. Sardinas, Joseph L. and Jeannine D. Muldoon. “Securing the Transmission and Storage of Medical Information.” *Computers in Nursing* 16, no. 3 (1998): 162-168.

20. American Bar Association Section of Science and Technology Information Security Committee. “Digital Signature Guidelines Tutorial.” American Bar Association. Available online at www.abanet.org/scitech/ec/isc/dsg-tutorial.html.

21. *Secrets & Lies: Digital Security in a Networked World*.

Reference

Dennis, Jill C. “The New Privacy Officer's Game Plan.” *Journal of AHIMA* 72, no. 2 (2001): 33-37.

Joseph L. Sardinas Jr. *(jlsjr@home.com) is a professor in the department of accounting and information systems at the Isenberg School of Management, University of Massachusetts.* ***Jeannine D. Muldoon*** *(muldooj@sunyit.edu) is dean and professor of the School of Nursing at the State University of New York Institute of Technology at Utica/Rome.*

Article citation:
Sardinas, Joseph L., Jr. and Jeannine D. Muldoon. "Are You Vulnerable to Hackers?: How to Protect Patient Information." *Journal of AHIMA* 72, no.10 (2001): 47-53.