BLUE ORANGE® COMPLIANCE

Cybersecurity in the Healthcare Arena

Introduction

With healthcare security breaches making all-too-frequent headlines, the threat of malicious hacking is a reality for every provider. The Health Insurance Portability and Accountability Act (HIPAA) requires covered entities and their business associates to safeguard against reasonably anticipated threats to Protected Health Information (PHI). Healthcare providers must institute administrative, physical, technical, and organizational safeguards to protect against unauthorized use and disclosure of PHI. However, HIPAA compliance alone does not necessarily make an organization immune to a cyberattack.

According to the 2018 end-of-year Breach Report compiled by the Identity Theft Resource Center (ITRC), the healthcare sector ranked second in number breaches and first for rate of exposure per breach. Criminals have developed increased proficiency in identifying and exploiting security vulnerabilities in healthcare IT security. Environments that have addressed HIPAA regulatory compliance may have additional work to do to secure their systems.

The Cost of a Data Breach

Cyberattacks have cost healthcare providers millions of dollars in regulatory fines, credit monitoring fees, attorney fees, and ransom charges. In the 2018 Ponemon Institute study, it was determined the average total cost of data breaches was $3.86 million, up 6.4 percent from the prior year. Criminal attacks on healthcare data are up 125 percent in the last five years, with healthcare data breaches costing organizations $408 per record—the highest of any industry.

In addition to the cost, a breach brings an organization under the scrutiny of the Office of Civil Rights (OCR), generates negative publicity, and compromises the welfare of a provider's patients and other stakeholders. In this cyberwar landscape, healthcare organizations have a legal and ethical responsibility to identify and mitigate the likelihood of real-world threats to IT assets and physical security.

The Best Defense

A healthcare provider's best defense is to recognize that no organization is impervious to cyberattacks. The number of incidents that evade traditional security defenses is increasing at an alarming rate. Moreover, the growing prevalence of Electronic Health Records (EHRs) has made the playing field even more enticing to scammers. True cybersecurity requires preparation, vigilance, and a proactive game plan.

Published: June 1, 2019

The Cybercriminal

Mindset and Methods

Cybercriminals are those who exploit computer weaknesses for financial gain or for fame. Hundreds of times per day, hackers worldwide are using the internet to probe IT infrastructure in search of vulnerabilities. These touches are conducted with methods so sophisticated that the hackers can hide their intentions. Their objective is the exploitation and collection of sensitive data that can be used for either profit or bragging rights.

Understanding both the mindset and practices of a hacker can help to better prepare defenses. While no two hackers are alike, hackers generally fall into two categories. The first category hacks as a hobby, often motivated by an ideological cause or the thrill of outsmarting their victims. The second practices hacking for strictly financial motives.

Hackers typically use the following process to select their targets:

Reconnaissance. Hackers begin by researching public information about an organization to identify potentially lucrative victims.

Scan. Once a target is selected, hackers will use various forms of software and hardware to evaluate and confirm the selection. These attempts are typically undetected by the target.

Gain Access. Hackers then employ malware on entry points to infect computers and other devices on the infrastructure.

Maintain Access. Hackers maintain entry points to allow continued access.

Cover Tracks. Hackers typically bury their tools deep within the network to allow continued access through a back door and are often able to remove traces of their attack altogether.

Points of Entry

Healthcare providers are under attack from all directions with hackers using many different tactics to gain access to an organization's system. Entry points could include mobile devices, USB drives, the internet, social media, email, and cloud and network infrastructures. A strong cybersecurity program will include layers to address and defend all entry points.

The Dark Web

The dark web, or deep web, is a layer of the internet that is not indexed by standard search engines where users can remain anonymous, share unlawful information, and conduct illegal business transactions. Because users are virtually untraceable, they are difficult to identify or monitor. PHI is a lucrative target for hackers because it provides huge payoffs on the dark web, where hackers can openly promote their stolen wares.

Published: June 1, 2019

Cryptocurrency

Cryptocurrency is an unregulated universal currency created for online, anonymous transactions. Bitcoin is the most commonly used cryptocurrency. While bitcoin is used for legal transactions, hackers also use this currency to buy and sell their wares. When hackers engage in ransomware attacks, payment is demanded in cryptocurrency as it leaves no trail back to the hacker.

Cybercrime Tools and Tactics

Malware

Malicious software, also known as malware, is any software designed to disrupt computer operations, collect confidential or sensitive information, or gain unauthorized access to computer systems. Malware is the tool of choice for most hackers.

How Malware Works

Malware can be a virus, application, or any unwanted software that gets installed on a computer or mobile device without the user's consent. Malware is typically installed when a user clicks on a link in an email (rather than typing the URL of a trusted site directly into a browser), opens an e-mail attachment, or browses to an infected website. Hackers also bundle malware with popular free downloads.

Popular Forms of Malware

Virus

A virus is a form of malware that infects programs and data files. Viruses can be transmitted as attachments to an email, in a downloaded file, or through external devices.

Worm

A worm is a malicious payload that can infect operating systems. Worms are designed to replicate themselves through a network or organization without additional input or guidance from the hacker. While worms can infect a system when a user clicks on an attachment, they can also propagate as a result of network vulnerabilities, infected file shares, links to infected websites, and other creative methods.

Spyware

Spyware is a type of malware that collects information or takes control of a computer without the user's consent or knowledge. Spyware can monitor a user's computer habits as well as detect and gather sensitive data. Cybercriminals may also piggyback spyware onto legitimate software. The presence of spyware is typically hidden and can be difficult to detect.

Keylogger

A keylogger is an application that records keystrokes on an affected computer. Hackers then use the information captured to gain access to passwords or other confidential information.

Published: June 1, 2019

Botnet
The term "botnet" is blend of the words "robot" and "network." A "bot" is a form of malware that infects a computer, remaining hidden until commanded by a hacker to complete a task. Hackers distribute bots across the internet in search of unprotected computers to infect. Once a series of computers has been infected, a "botnet" has been created. Hackers typically use botnets to transmit additional content, circulate spam, steal sensitive personal information, and generate denial of service attacks.

Ransomware
Ransomware is a type of malware that restricts access to the infected computer system, followed by demands that the user pay a ransom to the malware operators to remove the restriction. This is the only type of malware designed to notify a user that the infection has occurred. Once the ransomware has locked the files, it will announce what it has done, and communicate ransom demands.

Trojan
A Trojan is used to install malware, but typically does nothing else of ill intent. Trojans are often disguised as legitimate software and used by hackers to create a "backdoor" into a system that can later be used to gain access. Ransomware usually propagates with a Trojan.

Cryptojacking
In 2018, the practice of cryptojacking systems surpassed the use of ransomware. Unlike ransomware, the aim of the hacker running a cryptojacking campaign is to remain unnoticed for as long as possible. It begins when a user's computer is infected with malware designed to generate or mine cryptocurrencies such as bitcoin, litecoin, or monero. The longer the malware goes unnoticed, the longer the hacker can use the system to keep mining the cryptocurrency, creating a higher payoff.

A machine can become infected with cryptojacking malware from many of the same sources as traditional malware, including browser-based infections, phishing campaigns, or existing vulnerabilities on enterprise networks. Even when the source of the infection is determined or malware is detected, the path leading back to the hacker is virtually untraceable.

Cryptojacking malware can be a strain on system resources, causing slower performance, system overheating, and higher utility costs. In extreme scenarios, the malware can overwhelm system resources and disable the system altogether.

Vulnerability and Port Scanners

Vulnerability and port scanners are used to decide where to attack, however they do not breach anything on their own. A vulnerability scanner is a tool that can quickly assess computers on a network in an attempt to identify vulnerabilities. Port scanners check which ports on an individual computer are available to access. Both tools can be used by hackers to identify potential entry points. These products should also be used regularly in a defensive cybersecurity program to identify vulnerabilities for intervention.

Published: June 1, 2019

Packet Sniffers

Packet sniffers are pieces of hardware or software designed to monitor network traffic—between computers on a network, as well as between networked computers and the internet. Similar in concept to a "wiretap" on a phone line, packet sniffers can capture passwords and other data while in transit over a network.

Password Attack Techniques

Password attacks are processes used by hackers to discover passwords for a system or organization. Some common password attacks include:

- **Brute Force.** Attempting to crack or guess a password by trying as many possibilities as time and resources permit.
- **Dictionary or Library Attack.** Attempting to crack a password using an electronic dictionary list or list of commonly used passwords.
- **Social Engineering.** Gaining the trust of someone and getting them to give access to their password. Methods may include phishing and telephone calls.
- **Malware.** Spyware that gets installed on a computer that monitors all keystrokes and reports back to the hacker.
- **Password Spray.** Attempting to gain access to a list of accounts/usernames by using a list of commonly used passwords.
- C**redential Stuffing.** Compromised username and password combinations are injected into various online accounts until a match is found. The account is then available for the hacker's use.
- **Pass the Hash.** An attack that allows the hacker to gain access to a user account using only the password hash. A password hash is the system-level conversion of a user password to a string of characters that cannot be directly reversed into the password. The technique does not involve decrypting the hash or the password but allows the user to convince the system that the hash it is passing belongs to the account they are attempting to access.

Social Engineering

Social engineering is the manipulation of the natural human tendency to trust and avoid conflict, with the objective of gaining access to sensitive information. Using social engineering, a hacker may pose as a trustworthy contact to get the victim to do something outside of normal operations, such as disclose a password. The hacker will typically ask for just a little information at a time so that the encounter remains comfortable for the victim and a trust bond is developed.

These encounters can occur over the phone or online, with hackers often posing as a person of authority such as a network administrator, technical support representative, or an employee from a trusted vendor. Help desks can be particularly vulnerable to social engineering because those employees are trained to provide information

Published: June 1, 2019

and assistance. While some hackers use social engineering as their primary tactic, others may resort to it as an alternate strategy if the IT system of their intended victim is configured too securely.

It is sometimes difficult to recognize real-life examples of social engineering attacks because the crime is not easily traced. The employee that was victimized may not realize he/she disclosed sensitive information to an untrustworthy source or may be unwilling to admit the disclosure, hence the incident goes unreported. Moreover, social engineering breaches often leave no physical evidence or an easily identifiable entry point so, if a breach does occur, the method may remain a mystery.

Phishing

Phishing, a form of social engineering, is an attempt to acquire sensitive information such as usernames, passwords, bank account information, credit card details, and social security numbers by masquerading as a trustworthy entity. As our society shifts to relying more on electronic communication, phishing attacks are becoming increasingly effective and widespread.

As companies shore up their security footprints, hackers are forced to be more creative to get in. They will often try to prey on unsuspecting or unknowing users who they hope are too busy to pay attention to the details. Phishing attacks are effective largely because they convince the recipient to bypass critical thinking. A prize needs to be claimed immediately or there is a problem with a user's account that must be dealt with. Phishing attacks push users into thinking emotionally and acting without thinking.

How Phishing Works

A phishing scam is typically carried out with the help of an unsolicited email or a fake website that poses as a legitimate site to lure in potential victims and prompt them to provide valuable personal or financial information, system user IDs, and/or passwords. Newer phishing attempts involve incoming phone calls where the hacker poses as a representative of a known vendor. They claim they haven't been paid for a past due invoice, and are trying to get someone unsuspecting to wire them payment or provide financial information, check routing numbers, etc. Armed with this information, a criminal can commit identity or financial theft.

Phishing emails often target unaware end users, tempting the user to click on a link or attachment that will ultimately download spyware. Scammers craft their emails and web pages carefully, often copying web page layouts and logos of the entity they are trying to impersonate.

Phishing Prevention

Educate employees on the mechanics of phishing

- Be very wary of any unexpected email asking to click links, open attachments, or download files—especially if financial or other private information is requested.
- Do not provide personal information or information about the organization, including its structure, networks, or log-in credentials unless certain of a person's identity.
- If spelling or grammatical errors are noticed, be extremely cautious of the validity of the email.

Published: June 1, 2019

- Look for 'https://' and a lock icon in the address bar before entering any private information.
- Don't click a link from an email message and don't copy a link from an email message to paste into a web browser. Phishers can make links appear to go to one place, but then actually direct victims to a different site. For example, when receiving an email from LinkedIn, type www.linkedin.com into a browser or use a known bookmark.
- Don't send personal or financial information by unencrypted email.
- Have a firewall and an updated anti-virus program that can scan emails.
- Remember, the best way to remain protected is to STOP and THINK before you CLICK.

Spear Phishing

Spear phishing is a targeted phishing campaign typically sent randomly to a set of users, generally with no ties to one another. A spear phishing campaign is a directed attack with a specific target and goal in mind—and often a higher payoff for the hacker.

How Spear Phishing Works

In spear phishing, a target is selected such as a specific company, a department within the company, or an individual employee of the company. Unlike a typical phishing campaign, the target is not random. Careful thought and planning go into selecting the target.

The hacker will then collect information about the target. Social engineering, social media accounts, corporate websites, press releases, and information from the dark web are all resources at the hacker's disposal.

With the appropriate amount of information, the hacker will release the targeted attack, generally in the form of an email sent directly to the individual target. The email will appear to be sent from a trusted source such as a spouse, relative, or company executive and will be crafted in a way to elicit an emotional response with the goal of getting the recipient to either open an attachment in the email or click through to a website and enter sensitive credentials.

Once the payload has been delivered (the attachment was opened or the link was clicked), the hacker is free to continue the exploit and collect the sensitive information they were after.

Spear Phishing Prevention

Because spear phishing is a targeted attack, hackers will go to great lengths to cover their tracks and prevent detection than they would with a typical phishing attack. The techniques used to prevent phishing attacks also apply to prevention of spear phishing. Additionally, employees should be aware that if an email from a trusted source seems unusual or out of the ordinary, a quick phone call to the sender to verify the contents can be the difference that stops a spear phishing attack.

Published: June 1, 2019

Whaling

Like phishing, whaling is an attempt to acquire sensitive information by masquerading as a trustworthy entity. But in this crime, the targets are typically executive or C-level employees who have access to high-level PHI or financial data.

How Whaling Works

Hackers use various forms of social engineering to gain information about high-level employees. Armed with this information, hackers will disguise themselves as a trusted entity in an attempt to acquire financial information or sensitive data. Hackers may even use social media to determine when a high-level employee is on vacation and then contact his or her assistant.

Whaling Prevention

Whaling prevention techniques are similar to phishing prevention techniques (see above). In this case however, it is imperative that executive-level employees are educated on the possibility of these scams.

Cybersecurity Best Practices

Identify

The first step to arming an organization against cyber threats is to conduct appropriate inventory management and testing to know the environment and the risks that need to be addressed.

Recognize the Risk

No infrastructure is immune to cybercrime and with the growing prevalence of EHR, security breaches against healthcare organizations are on the rise. The best strategy is to recognize the risk and adopt a course of action that proactively defends, detects, and denies attacks.

Conduct Regular Security Risk Analyses

Routine security risk analyses will identify potential cybersecurity vulnerabilities as well as better position a healthcare organization for an audit. A thorough and accurate risk analysis will address all 60+ applicable areas of the HIPAA Security Rule.

Perform a Tabletop Exercise

Once policies and procedures are in place, simulate a security incident to determine how the organization would fare if the incident occurred. Tabletop exercises reveal weaknesses in communication or policies and procedures, and provide good indications of areas to address and correct. Exercises may be conducted to focus on specific areas like security incident response or contingency planning.

Published: June 1, 2019

Perform Penetration Testing

Penetration testing, also known as "ethical hacking," is an authorized attack on a computer system designed to identify security vulnerabilities in operating systems, applications, configurations, or end-user activity. The cost of penetration testing is justified by considering the impact to the organization if an attacker were to successfully gain access to sensitive data. Implementation of routine penetration testing followed by remediation of identified vulnerabilities can strategically position an organization to discourage cyberattacks.

How it works. A penetration test utilizes the practices and methods of external or internal agents attempting to gain unauthorized access. A tester will employ realistic methods to attack users and systems to accomplish agreed-upon goals.

A thorough penetration test uses the latest software tools designed to gather information, analyze and exploit vulnerabilities, crack passwords, or leverage weaknesses in web applications and wireless networks. The primary objective is to establish where system access can be attained. Once security gaps are identified, they should be corrected, and subsequent tests executed. While there will never be a zero-vulnerability situation, organizations should strive to be able to detect and respond to an attack while making sure to be a harder target than their peers.

Protect

Key to a successful cybersecurity program is developing and implementing controls. Preventing or reducing the chance of identified risks occurring is a major step toward cybersecurity.

Conduct Security Awareness Training

For all the safeguards afforded by software and technology, humans continue to be the most exploitable vulnerability in the cybersecurity landscape. Employee carelessness, forgetfulness, and lack of knowledge can create a huge gap in an otherwise secure setting. This gap can make an organization highly susceptible to a cyberattack, security breach, and ransomware. It can also put an organization at risk for costly HIPAA violations that could generate negative publicity and reputational damage.

As a healthcare provider, HIPAA law requires covered entities to conduct workforce security awareness training. In addition to achieving HIPAA compliance, this initiative can also provide stronger strategic positioning in the cyberwar arena. Since a company's workforce is often its first line of defense, a figurative human firewall, arm them with the proper—and ongoing—training for the battlefield.

Cultivate Workforce Security Awareness

Monitor and communicate industry security trends and vulnerabilities. Remain alert and informed on current and emerging threats. Provide periodic security updates and reminders to the workforce. Educate employees on the mechanics of spam, phishing, and malware. Test workforce awareness by initiating internal phishing expeditions to attempt to solicit information from employees.

Published: June 1, 2019

Encourage Employee Skepticism

Encourage employees to be vigilant and skeptical, adopting a "question everything" attitude. Ensure organization-wide clarity on the correct and timely reporting procedures for potential malicious social engineering or software threats.

Promote Log-In Vigilance

Train the workforce to detect inconsistencies with log-in procedures and recognize whether their accounts have been illicitly accessed. Develop a procedure for employees to report log-in anomalies and consistently stress the importance of log-in vigilance. Implement technical safeguards that allow for the monitoring and investigating of suspicious log-in activity. Audit and monitor system users.

Limit Access to ePHI

Limit access to Electronic Protected Health Information (ePHI) exclusively to persons or software programs that absolutely require access. This access should only be provided when it can be individualized and tracked.

Encrypt ePHI

Encryption uses mathematical formulas to scramble data, making the sensitive details desirable to hackers unreadable without a decryption key or code. Encrypting data can prevent sensitive information from being compromised in transit or at rest. Encryption is a critical step due to the high incidence of lost or stolen disks, tapes, laptops, USB storage devices, and smartphones.

Mitigate Mobile Device Exposure

Common points of hacker entry often involve mobile devices. To mitigate exposure:

- Require password protection on all mobile devices.
- Use data encryption on mobile devices. Hackers often steal these devices as "the way in," and if a single device is compromised, the EHRs on the server could be at risk.
- Install remote wiping features to provide a second line of defense to encryption. If a device is lost or stolen, sensitive data can be erased remotely.

THE KEY TO PASSWORDS

Passwords provide the keys to the systems that contain sensitive data. Taking the time to create more complex passwords may seem to be an increased burden initially, but strong passwords make it harder for the hacker to gain access to systems and data within the organization.

Length. The character length of a password has been shown to significantly impact the ability to guess or crack an account password. Extending the length of the password to higher character minimums through passphrases or word combinations proves to be a stronger method for security.

Prevention. Organizations implementing a minimum password length and complexity requirement can prevent their users from setting weak passwords. Password filtering, which prevents commonly known bad passwords, regular components of bad passwords, and organization specific words, is another way that organizations can prevent users from setting a bad password in the first place.

Detection. Requiring multifactor authentication (MFA) on external logins is one way to gain visibility if an attempt is being made to use a password maliciously. Having appropriate log aggregation to monitor failed attempts or abnormal user login attempts is another way to go beyond simply relying on a strong password to ensure that sensitive data is protected.

Published: June 1, 2019

- Develop, implement, and enforce a comprehensive set of policies and procedures related to the use of mobile devices in the workplace.

Maintain Firewall Protection

A firewall will mitigate a system's exposure to hacker intrusion by evaluating data coming in or going out against a set of security rules an organization assigns. Best practice is to frequently review firewall logs and settings, with a hard focus on intrusion detection and prevention. Firewalls should be used on individual devices and at network edges.

Detect

Once protection measures are in place, it is important to have the ability to detect potential breaches. Maintain antimalware and actively manage access logs. Regularly review these systems to detect active threats.

Monitor Data Movement in the EHR System

Scrutinize physical and system access. Configure systems to log events that are required for security and compliance. Regularly review and analyze logs for indications of suspicious behavior. In short, implement and practice a vigilant monitoring system that allows for the immediate and continual identification and investigation of abnormalities.

Malware Detection

Malware is difficult to detect because hackers go to great lengths to ensure their malicious software goes unnoticed and does not impact system performance. However, a computer may be infected with malware if it runs slowly, displays continual error messages, exhibits web pages not searched for, or displays repeated pop-up messages. Additional signs include changes in the computer's browser, such as unfamiliar tabs or a different default search engine. Again, while those signs typically mean something is wrong, the malware is often undetectable.

MALWARE PREVENTION

- **Scan USBs and other external devices before using them.**
- **Purchase software directly from the source to avoid installing software that has been "bundled" with a virus.**
- **Install malware detection software and ensure anti-virus software is in place. Keep both up to date.**
- **Use a firewall and frequently review firewall logs and settings.**
- **Educate employees on the mechanics of malware.**
- **Remain alert and informed on current and emerging threats, providing periodic security updates and reminders to the workforce.**
  - **Avoid opening email attachments that are not from a confirmed and trusted source.**
  - **Avoid clicking on a link in an email, and instead type a trusted URL address directly into a browser.**
  - **Avoid clicking on pop-ups and banner ads.**
  - **Do not change a browser's security settings.**
  - **Pay attention to browser security warnings. Many browsers provide a warning before a user visits an infected website or downloads a suspicious file.**

Published: June 1, 2019

Respond

A thorough and effective cybersecurity program must include having a response plan for detected threats, attacks, or unauthorized access. Leverage a variety of tactics to optimize communication and minimize recovery time.

Resolve or Contain the Issue

Follow established plans to stop unauthorized access or detected attacks. Conduct investigations and gather evidence to facilitate required notifications and ensure the entire threat has been resolved.

Know Who to Call

A good response plan will include details on when to contact each internal resource and which external resources are available for additional support and guidance. Having this information documented ahead of time ensures that the right people are kept in the loop and that any available support is deployed promptly.

Know What to Say

Unpleasant as it may be, determine when it is appropriate to write a press release or breach notification. A well-documented plan will include who to notify, when to notify, and what that notification should say.

Keep Improving

Don't make the mistake of thinking that having a plan is enough. Ensure that there are proper steps to regularly review the plan's effectiveness and update processes when required. Process improvement should span all parts of a cybersecurity program.

Recover

Should a breach occur—and once mitigation and remediation are addressed—it is important to restore operating capabilities, backups, and other recovery solutions as swiftly as possible. Develop systems and a detailed plan so that the process is smooth, thorough, and timely.

Regular System Backups

Perform frequent and comprehensive system backups to ensure business continuity and disaster recovery. Keep tiers of data backups stored in different locations or mediums. A backup copy should be kept offline and another copy kept offsite. Routinely copy recovery points to a USB disk or other offline media.

Maintain a Contingency Plan

Having a comprehensive contingency plan that includes disaster recovery, emergency operations, frequent data backups, and test restorations is crucial to ensuring business continuity.

Published: June 1, 2019

Cyberattacks are an ongoing and ever-evolving threat to healthcare providers. In addition to the cost, a breach can trigger federal investigation and damage to the organization's reputation. The key is to be prepared. Develop a system for protecting, detecting, responding, and recovering from cyber threats. With a solid system in place, a provider can prevent attacks and mitigate the effects if breaches should they occur.

To learn how BlueOrange Compliance helps healthcare organizations to protect against cyber threats, request a free consult. Call 855.500.6272 or visit www.blueorangecompliance.com.

About BlueOrange Compliance:

BlueOrange Compliance specializes in assisting healthcare organizations navigate HIPAA and HITECH privacy and security requirements. Complex, ever-changing healthcare regulations and increasing risks make it difficult for organizations to stay in front of emerging cyber threats. As a single source, we equip every client with affordable, practical, comprehensive privacy and security solutions, including multiple sources of information to help manage risk. Our clients have peace of mind knowing they are compliant and prepared for potential breaches and adverse audits.

Published: June 1, 2019