DIGITAL GUARDIAN®

6 InfoSec Pros on the Top Healthcare Security Considerations

Introduction

Healthcare organizations face numerous risks to security, from ransomware to inadequately secured IoT devices and, of course, the ever-present human element. Coupled with HIPAA and other regulatory requirements that make securing protected health information (PHI) paramount, healthcare organizations have no shortage of serious security considerations that must be adequately addressed to ensure patient privacy and safety.

To find out what security considerations are weighing heaviest on the minds of healthcare security pros, we reached out to a panel of security professionals and asked them to weigh in on this question:

"What are the top 3 information security considerations for healthcare organizations?"

Read on to find out what our panel had to say.

Mike Meikle

@mike_meikle

Mike Meikle is a Partner at SecureHIM, a healthcare security consulting and education company. SecureHIM provides cyber security training for healthcare clients on topics such as data privacy and how to minimize the risk of data breaches. They also provide extensive cybersecurity consulting services for their customers.

“The top three information security concerns for healthcare (mobile, EMR, ransomware) all revolve around the protection of Electronic Protected Health Information (ePHI).

State and federal privacy and security guidelines such as HIPAA directly impact the ramifications of a data breach which can result in significant penalties for an institution.
Mobile devices have opened a large attack surface on healthcare data assets. While mobile device usage has changed the way healthcare conducts business, it has come at a significant price of additional vulnerability to cyber-attacks. The added pressure of meaningful use mandates and consumerization (BYOD) trends of mobile devices into the practice is pushing healthcare to adapt new workflows and business models. Risk mitigation must be a primary concern as this trend continues.

Ransomware has exponentially increased as a threat to healthcare. The attacks cannot be wholly stopped or prevented, no matter what type of technological and personnel controls are implemented. If a malicious actor wants to break into a person’s or company's sensitive information, they will find a way. It may not be a technical approach; it could be using very reliable social engineering techniques.

Ransomware relies upon technical and personnel vulnerabilities that are growing in scope and visibility due to the increasing automation and interconnectedness of systems, mobile devices and the sharing of personal data. The financial incentive is there for the criminal, nation-state, or other malicious actors to perpetrate these crimes.

Mike Meikle (Cont.)

@mike_meikle

The most effective way to recover from a ransomware attack is to have a well-tested backup and recovery plan for your organization. If the organization can roll back their saved data to a time when the ransomware had not infiltrated the organization, then there should be minimal financial loss.

Health and Human Services Office of Civil Rights has stated that successful ransomware attacks that occur in a healthcare organization are considered a data breach and must be reported.

The protection of intellectual property (IP) and Electronic Patient Health Information (ePHI) is the driving force behind EMR security. A large percentage of EMR systems are cloud based. If a cloud service provider stores information in overseas data centers it may not be protected by U.S. intellectual property laws and therefore it may be difficult to prove the confidentiality and integrity of a customer's or patient's data. Industries that put additional privacy and security burdens on data protection such as healthcare have additional regulatory burdens to consider.

As the reliance on cloud services grows larger, the security evaluation of these services grows in importance. How do you evaluate the security risk in using such a service? What important security questions should be asked? The first step is to query the Cloud Service Provider (CSP) on what security auditing standards their services comply with (SAS 70, FIPS 200, etc). Consider where the data will be stored and if U.S. IP laws will apply. Review the contract language, terms and conditions for appropriate risk management on behalf of the CSP or third-party. CSPs will also have to sign a Business Associates Agreement (BAA) per HIPAA privacy and security guidelines."

Will Durkee

@SCAdvantage

Will Durkee is Director of Security Solutions for TSC Advantage, an enterprise cyber risk and cybersecurity consulting firm that works with Fortune 500 companies in healthcare and other critical infrastructure sectors to provide an objective understanding of security posture and prioritize resources for a proactive and holistic defense. Will holds CISSP and HCISSP certifications. TSC has been published or quoted in The Hill, Dark Reading, CSO, Security, ReadWrite, New York Times, Time, WSJ, and more.

"The top 3 information security considerations for healthcare organizations are...

1. **Focus on the human –** Human error is attributed to numerous breaches from phishing emails to misplaced PHI storage devices. The evidence shows that people continue to be a weak link in protecting the security of information. Adversaries use increasingly sophisticated methods to trick employees into clicking on malware-infested emails or to request fraudulent transfers of funds; and disgruntled or malicious insiders may knowingly steal or sabotage assets or systems.
2. **Track what goes where –** Patient information can flow through a complex network of multiple healthcare providers, specialists, bill payment processing firms, insurance payers, etc. Healthcare organizations need to track all steps this confidential information takes and ensure security during each phase. Many HIPAA breaches are caused by lost or stolen devices that contain Protected Health Information (PHI). As PHI devices multiply swiftly, the risk of breaches and stress of keeping track of devices increases.
3. **Ensure your partners play by your rules –** Adversaries are always looking for the path of least resistance, and that can often include use of third parties and supply chain partners to gain a foothold onto your network. Furthermore, a cybersecurity event affecting a critical vendor can lead to catastrophic interruptions to your business and profitability. The use of business associates is common, though implementing a third-party risk management process is still lagging. Ensure your information-sharing partners adhere to minimum security standards either through distributed security assessments or HIPAA Security attestations."

Mike Baker

@Mosaic451

Mike Baker is founder and Principal at Mosaic451, a bespoke cybersecurity service provider and consultancy with specific expertise in building, operating and defending some of the most highly-secure networks in North America.

“The biggest security considerations for healthcare organizations are…

1. Wearable and implantable IoT healthcare devices, from pacemakers to insulin pumps to monitors can be vulnerable to attack.
   Up until now, cybersecurity has been focused on computers and the networks they are connected to. However, the rapid proliferation of IoT devices, which includes pacemakers, insulin pumps and other devices, is quickly redefining the definition of a “computer,” and all of them are connected to the Internet. IoT devices tend to have weaker security protections than regular computers, including hard-coded and widely known passwords, and unlike computers, not all devices are easily patched or updatable. Additionally, there are many IoT device manufacturers, and the devices are sold through different channels; there are no common controls regarding passwords, encryption, or other security measures, and no “chain of custody” controls tracking who has handled the device or when.

   Recently, the healthcare industry has come under attack from ransomware, which hackers use to breach a system and render it inoperable until the victim pays a ransom. This scenario isn’t outside the realm of possibility. By locking medical providers out of patient medical records, hackers have demonstrated they have no qualms about putting the lives of innocent people at risk.

2. Buying technology alone is a security strategy that does not work. Insider threats present a huge security risk.

   Healthcare is under constant pressure to safeguard assets; however, too many firms focus on security for HIPAA compliance and then call

Mike Baker (Cont.)

@Mosaic451

it a day. Compliance is a legal necessity, but organizations expose themselves to cyberattacks when they use technology as a crutch. Many organizations will need to look at their operations as a critical network and seek ways to defend it. There is clearly a need for organizations to employ automated systems that continuously monitor the organization's network, establish a pattern of use for each individual user, alert security managers to any deviations from user patterns, and then require additional authentication before allowing the deviant action to proceed further – all while simultaneously alerting the IT security team.

Upon examining some of the largest healthcare data breaches, data was breached due to hackers successfully exploiting humans.

The proliferation of mobile devices in healthcare like smartphones and tablets have also made the human element even more vulnerable because this area of security is often overlooked and is in fact the weakest link. Technology is only as good as the people who use it and is merely a tool in the fight against cybercrime. Technology alone cannot fully protect an organization's data, networks, or interests.

3. DDOS attacks: an old nemesis returns to cripple your network.

Once considered a cybersecurity threat of the past, Distributed Denial of Service (DDoS) attacks have re-emerged with a vengeance. DDoS attacks are wreaking havoc on enterprises and end users with alarming frequency.

Distributed Denial of Service is a cyberattack where multiple systems are compromised, often joined with a Trojan, and used to target a single system to exhaust resources so that legitimate users are denied access to resources. Websites or other online resources become so overloaded with bogus traffic that they become unusable. A well-orchestrated DDoS carried out by automated bots or programs has the power to knock a website offline. These attacks can cripple even the most established and

Mike Baker (Cont.)

@Mosaic451

largest organizations. An e-commerce business can no longer conduct online transactions, jeopardizing sales. Emergency response services can no longer respond, putting lives in danger.

The reason why DDoS attacks are back is simple - it is relatively easy to launch a sustained attack and cripple any organization connected to the Internet. Botnets, a group of computers connected for malicious purposes, can actually be acquired as a DDoS for hire service. The ability to acquire destructive assets demonstrates how easy it is for someone with little technical knowledge to attack any organization.

Detecting a DDoS attack requires specialized hardware capable of sending alerts via email or text. The goal is to report and respond to the incident before the attacker makes resources unavailable. An MSSP who employs both technology and on-site personnel can monitor and act as a full operations team."

Shai Canaan

@Nettitude_com

Shai Canaan is a Security Consultant from cyber security consultancy Nettitude, Inc.

"For healthcare organizations, the top 3 information security concerns include...

1. **Inside threats via employee errors or lack of awareness -** employees are the soft belly of a well-defended IT infrastructure. Employee carelessness and lack of awareness may lead to a breach despite a solid network perimeter. Common examples are employees introducing threats via clicking on a malicious attachment in an email, or connecting their personal mobile device to the organization's Wi-Fi or hardware. Such threats can lead to an introduction of ransomware and malware which may harvest user credentials or even open a backdoor for a hacker.

2. **Data classification management -** targeted cyber-attacks are very difficult to detect and stop; however, how much the attackers may get depends on the organization's data management. When hackers successfully breach an organization they are commonly targeting the electronic protected health information (ePHI) stored in databases. Whether or not they will access this data usually depends on how well the data is classified and available to specific users based on business need-to-know. The better an organization understands its sensitive data flows, the better it can protect it.

3. **Defense in depth -** healthcare organizations should understand that there is no one layer of defense which they should rely on. Each layer of defense contributes a little more to the complexity of a breach and thus slows down attackers, resulting in some hackers moving on to an easier target. A freshly updated, well configured, and capable firewall will prevent a majority of simple attacks, but the more sophisticated ones will find their way in. Similarly employees may introduce threats from the

Shai Canaan (Cont.)

@Nettitude_com

inside, something which most firewalls will not be able to stop. Example of additional layers from a human resources angle can be periodic and effective employee awareness training. Another example from a technical standpoint is adding proper encryption to ePHI databases and applications which access ePHI. Such encryption may prevent a hacker, who may have already gained some internal access, from the ability to decrypt and thus expose ePHI."

Amit Kulkarni

@cognetyx

Amit Kulkarni is CEO of Cognetyx Corporation and a member of the company's board of directors. He co-founded Cognetyx, bringing more than 18 years of technology leadership, computer network security expertise, and executive management experience to his role with the company.

"The top 3 information security considerations for healthcare organizations are…

1. Artificial Intelligence is Now an Affordable Healthcare Security Option

   Artificial Intelligence (AI) technology is becoming commonplace in industries such as healthcare, which deal with large amounts of data or rely on low-risk repetitive tasks. Because of technological advances, the cost of a powerful AI security solution, which used to be only affordable to the largest organizations, can now fit the budget for almost any healthcare organization. Artificial Intelligence can offer automatic surveillance, detection and data breach alerts in real-time.

   Leveraging artificial intelligence and machine learning allows healthcare organizations to enjoy real time protection and risk identification, significantly reducing security risks without the need to increase staff.

2. Third Party Contractors: The Hacker's Backdoor

   Third party contractors, or Business Associates (BAs) are proving to be a similar headache for healthcare organizations. A 2016 study published by the Ponemon Institute found that in the prior two years 89% of healthcare organizations and 60% of their BAs had experienced some type of data breach. The problem is, no matter how robust the cybersecurity of a healthcare organization, as long as criminals can gain legitimate login credentials through third party vendors, they can still compromise the organization via this backdoor. The key here is that hackers can penetrate your site without gaining entry through the front-end login page. With an ever evolving ecosystem of hundreds of BAs providing a wide range of services from medical and administrative

Amit Kulkarni (Cont.)

@cognetyx

to facilities, these BAs represent a significant risk to healthcare organizations. Therefore, it is prudent for healthcare organizations to mitigate these risks as much as possible in order to protect internal systems, sensitive patient data and company reputation.

One method is to create assessment and evaluation criteria that would ensure all vendors have adequate cybersecurity within their own enterprise. Whether it is robust security software, up-to-date firewalls, or personnel training on security and data protection best practices, ensuring that BAs have the same robust standards of cybersecurity that healthcare organizations themselves have is a key way to minimize risk. Make sure that vendors pass security certifications that renew as needed, and periodically reassess for vulnerabilities.

As part of the assessment process, healthcare organizations should subject their BAs to vulnerability and penetration testing (VAPT) on both external and Internet-facing products, so that any vulnerability can be discovered and fixed before they can be exploited by hackers. Using a VAPT approach, an organization can get a more detailed picture of the threats that may face its systems, which enables the business to better protect its systems and data from hackers. Vulnerabilities as well as the potential for unauthorized access can be found in applications or security leaks from third party vendors. Those potential areas of backdoor access can typically be easily fixed once discovered while the VAPT provider continues to search for and classify vulnerabilities. Coupled with advanced cybersecurity technology to detect unauthorized and malicious users even when they use legitimate credentials, it is possible for healthcare organizations to inoculate themselves against cyberattacks.

3. Insider Threats Pose a Huge Security Risk for Healthcare

When people generally think of hacking, they visualize it as external criminals attempting to penetrate a network. The methods that get the most attention are malware or phishing scams. All of this feeds into the

Amit Kulkarni (Cont.)

@cognetyx

notion that to prevent attacks, we just need better defenses around the perimeter.

What if the attacker is already inside the network? Once inside, there's seemingly no way to either detect someone is up to no good, or to alert the proper authorities that something might be amiss. Any insider, knowingly or unknowingly, can put sensitive data at risk. There are two main types of insider risks that pose the biggest problem. The first is the "malicious insider." This type of person could certainly be an external hacker who has broken into the network, either from hacking or stolen login credentials. Even more concerning, it could be a current employee who is snooping in data that they shouldn't be in. The second is the "negligent insider", who due to ignorance and lack of knowledge, clicks on a phishing link and downloads malware.

Technology can stop a malicious insider once they are in. Technology is advancing at a rate where the convergence of progress in multiple areas is finally making it possible to detect malicious insiders. The cost of storing data continues to go down. The processing capabilities of servers to sift through data keeps marching forward, and advances in machine learning/artificial intelligence makes it possible to make sense of the data in meaningful ways."

Julian Jacobsen

@JJMicroLLC

Julian Jacobsen is a HIPAA compliance IT consultant and owner of J.J. Micro LLC IT Consulting. He supports over 120 clients in the St. Louis, MO area. Julian has over 10 years of consulting experience and specializes in small medical and dental practices.

“Healthcare organizations should be asking themselves three major questions…

Are we HIPAA compliant?

HIPAA audits are increasing, and fines are huge. In 2017, the OCR collected $19.4 million in fines, down from 2016’s $23.5 million but still up from 2015’s $6.2 million. The more fines the OCR hands out, the bigger their budget to perform audits grows. We are seeing small practices audited and fined just as often as larger organizations. It's important that small practices don't assume their size will hide them from the Office for Civil Rights. The rules that govern healthcare organizations are very different from other industries. What is good enough for other segments is not necessarily good enough for healthcare organizations. For instance, let’s look at data storage in the cloud. There are many cloud storage providers who are SOC 2 compliant and are very experienced at securely storing important data. The data is stored in an irreversibly encrypted way and the data center does not have the encryption key; so they can never access the data. If that cloud storage provider is unwilling to sign a Business Associate Agreement, PHI (Protected Health Information) cannot be stored there.

Do we have good ransomware protection?

Ransomware has been the fastest growing digital threat to the healthcare industry over the last two years. Ransomware continues to put protected health information at risk in organizations of all sizes from small practices to large hospitals. Remaining HIPAA compliant requires organizations to minimize these attack surfaces and train employees to spot ransomware attacks. This training can require a serious time investment from an

Julian Jacobsen (Cont.)

@JJMicroLLC

organization. However, from a compliance standpoint, this investment in time and labor will pay dividends if an organization can avoid a major HIPAA breach. In addition to training, a healthcare organization will need to invest in a multi-pronged approach to ransomware prevention. Advanced SPAM filtering to prevent phishing and spear phishing attacks (major vectors for ransomware), DNS filtering to block access to known malware sites, and deep packet inspection at the firewall level to search for malware signatures.

Do we have a solid backup strategy?

As a last fail-safe against ransomware and any other IT related disaster, an organization must have a comprehensive backup solution that takes into account the power of ransomware to encrypt any data the infected machine has access to. This can include network shares that aren't mapped as network drives. If backups are stored on a network share that can be accessed by workstations, those backups are at risk of being held at ransom with the rest of the data on the network. An organization must consider how it separates its local backups from the rest of the network. Additionally, an organization must have offsite backups stored in a geographically distinct and secure location. Healthcare organizations must also consider the frequency of their backups. Data stolen and data lost (but not stolen) are both considered HIPAA violations. A nightly backup might not be enough to ensure compliance.”

Like what you read?

Get more insights from additional InfoSec professionals on the top InfoSec considerations for healthcare organizations here:

https://digitalguardian.com/blog/healthcare-information-security-top-infosec-considerations-healthcare-organizations-today

DIGITAL GUARDIAN®

Questions?

1-781-788-8180
info@digitalguardian.com
www.digitalguardian.com

Click below to view additional resources

- KLAS Data Loss Prevention 2017 Report
- Stopping PHI Theft with DLP Real World Scenarios