Hackers, breaches, and the value of healthcare data

June 30, 2021 // Ellen Neveux (https://www.securelink.com/blog/author/eneveuxsecurelink-com/)

Last Updated: August 23, 2021

Healthcare data breaches are increasing exponentially year after year, and it doesn't seem like they're going to slow down any time soon. It's important for healthcare IT professionals to take steps to safeguard their systems, whether that means protecting against external threats (/products/securelink-for-healthcare/) posed by hackers and cyber criminals or securing internal threats that come from access abuse from internal users (/products/patient-privacy-monitoring/). **It's also critical for them to understand why healthcare data is vaulable for hackers and insider threats.**

By how much did healthcare data breaches increase in 2020?

27.5%

55.1%

70.3%

Why is healthcare data so valuable?

Healthcare data is valuable on the black market because it often contains all of an individual's personally identifiable information, as opposed to a single piece of information that may be found in a financial breach. Often these attacks see hundreds of thousands of patient's data and privacy compromised or stolen by those with malicious intent. According to a Trustwave report (https://www2.trustwave.com/Value-of-Data-Report_LP.html), a healthcare data record may be valued at up to $250 per record on the black market, **compared to $5.40 for the next highest value record (a payment card)**. Because of the desirability of the data and the lure of monetary gain, it is important that this security threat is not underestimated by healthcare industry IT professionals and that steps are taken to safeguard this data.

Most of these breaches can be attributed to criminal insiders and hackers gaining access through third-party vendors. The Ponemon Institute found that the costs associated with remediating a breach are estimated at $740,000 (/blog/hospitals-spend-more-after-data-breach-but-there-is-a-fix/), and if a third party causes a data breach, the cost of the attack increases by more than $370,000 (https://securityscorecard.com/blog/5-data-breach-statistics-and-trends-to-look-out-for-in-2020). Research suggests the attack vectors are most likely to be ransomware (a new favorite tactic (/ebooks/anatomy-data-breach-part-1/) used in recent attacks like the Colonial Pipeline and JBS USA

cyberattacks), or SQL injection attacks that can occur when malicious emails,

Related Posts

Hospitals spend more after data breach, but there is a fix (https://www.securelink.com/blog/hospitals-spend-more-after-data-breach-but-there-is-a-fix/)

EMR Access Monitoring: Focusing On What's Important (https://www.securelink.com/blog/emr-access-monitoring-focusing-whats-important/)

HIPAA compliance: What healthcare administrators need to know (https://www.securelink.com/blog/hipaa-compliance-what-healthcare-administrators-need-to-know/)

Related Resources

EMR Access Monitoring Checklist (https://www.securelink.com/checklist/emr-access-monitoring-checklist/)

Ultimate Guide to Third-Party Remote Access: Healthcare (https://www.securelink.com/guides/ultimate-guide-to-third-party-remote-access-healthcare/)

Allscripts Boosts Efficiency (https://www.securelink.com/case-studies/allscripts-case-study/)

Categories

Industry Compliance (https://www.securelink.com/blog/category/compliance/)

Industry Insights (https://www.securelink.com/blog/category/insights/)

Security (https://www.securelink.com/blog/category

websites, or software is installed or accessed within a network, often by an unsuspecting user.

Seeing this should be a wake-up call, and believe me, it's easy to see frightening information like this and want to duck and cover. But we all know that duck and cover practices are ineffective and wouldn't save anyone; it only makes an actual issue less frightening. **Instead, we're going to impart some real actionable advice on how healthcare IT professionals can defend against internal and external threats.**

Recent data breaches in the healthcare industry

The healthcare industry is particularly vulnerable to malicious ransomware attacks, and those vulnerabilities were exposed in the attack against Hancock Health in January 2018. According to Healthcare IT News (http://www.healthcareitnews.com/news/ransomware-attack-hancock-health-drives-providers-pen-and-paper), the attack was sophisticated, calculating, and motivated by financial gain. The attack forced the hospital's IT staff to shut down their systems while their patient's personally identifiable information was held hostage.

The Hancock Health breach was traced back to a hacker who used a third party's remote access portal and credentials, which are both leading causes of cyberattacks. The hospital was later compelled by the attacker to pay $55,000 using the cryptocurrency bitcoin in order to release the healthcare data.

Similarly, in May 2019, the American Medical Collection Agency (AMCA), a "business associate (/blog/risks-of-business-associates-and-hipaa-compliance/)" (or third party) of a number of healthcare providers, reported that an eight-month data breach exposed data and sensitive information of more than 20 million patients. The event brought into sharp focus (https://www.cpomagazine.com/cyber-security/amca-healthcare-data-breach-could-set-a-new-precedent-for-health-it-security/) the risks facing healthcare providers who depend on outside vendors for support services.

Under the Health Insurance Portability and Accountability Act (HIPAA) (/brochures/hipaa-and-hitech-brochure/), healthcare providers — also referred to as "covered entities" — can share protected health care information with vendors and business associates. Business associates can be anything from claims processors, bill collectors, accounting firms, consultants, attorneys, claims clearinghouses, and medical transcriptionists. **While third parties can offer more operation-critical services, they do require** remote access (/solutions/secure-remote-access-for-all-third-parties/) **to your network and sensitive data,** which, of course, makes them a huge threat to healthcare organizations (/industries/healthcare/).

Lastly (but certainly not least), the healthcare industry took an even bigger hit

during the COVID-19 pandemic. Hospitals were reaching max capacity, and the large amount of high-risk patient data put electronic medical records (EMR) in danger of being breached by hackers or users with malintent.

The best ways to prevent similar attacks against your institution are practical defensive solutions. **The IT healthcare professional needs to be prepared and know who is accessing their company resources from employees to third-party vendors and up.** Once you know how many threats or risks you are dealing with, the better equipped you are to build the tactical defenses needed to protect patient privacy and data.

What makes the healthcare industry vulnerable to data breaches?

Because of the number of interconnected devices in healthcare, opportunistic attacks are becoming more and more commonplace because there is a need for an organization to share information across devices and with third-party vendors. A network's integrity is weakened by these third parties, who may have access to a site's data through a vulnerable VPN (/blog/vpn-problems/) or multiple shared credentials. VPNs have no way of restricting the permissions of users who shouldn't have access to an entire network, nor do they have the capability to protect credentials if they've been shared.

Email is another vector for hackers to use via a third party's access. Attackers are aware that email is often a weak spot and will use this to take advantage by using phishing attempts to gain entry to a third-party vendor's vetted, yet still unsecure, network access.

And, of course, hackers can get a lot of data on a single person when targeting a healthcare facility. **Sure, credit card information is great; but ePHI is even better.**

The true danger of hackers targeting healthcare facilities lies in the urgency of healthcare staff needing access to patient files on the spot. It's the nature of the job to access medical records in an instant, so there isn't any time to wait for an access request to be approved. In some cases, it literally could be a matter of life and death. Hackers who target healthcare facilities know that once they gain access through VPN, credentials, or phishing, there's no way to restrict access to the information they've encountered. Once that door has been opened, it's unlimited and unrestricted access to dozens, hundreds, or even thousands of patient files – a goldmine for hackers.

How to protect healthcare data

First of all, we're not descending into Mad Max times. It's not yet a lawless wasteland. **While there is an undeniable proliferation of attacks and an increase in healthcare data breaches (a number that only seems to be rising), it is possible for IT professionals to defend against any rampaging apocalyptic marauders.**

Healthcare IT departments need to act as if a threat to their network and ePHI is imminent and respond as such – from both internal and external sources. Ultimately, a network is more secure when all individuals accessing the network can be identified and tracked. **It's important to have clear** network visibility (/why-choose-securelink/visibility-via-audit/) **to know who is on your network, when they're on your network, why they are on your network, and** what they did while they were on your network (/solutions/record-and-audit-sessions/)**.**

As an IT professional, it also behooves you to establish a praxis where all of

your access points are monitored and secure, as well as ensuring each employee, client, vendor, or end-user only has the least amount of access required (/solutions/least-privileged-access-for-vendors/) to do business.

Doing the above first requires you to assess your current company policies and identify areas of weakness. And look closely – sometimes those areas of weakness could be your own employees. In some cases, internal sources are the ones stealing ePHI and selling it on the black market, making access auditing an even more pressing and important player in patient data security.

However, simply looking within the organization isn't enough. **As a healthcare IT support professional, it falls on you to look at external relationships and work to shore up all potential weaknesses in these third-party relationships.**

It is important to be aware that the best protection against a healthcare data breach or attack (/blog/the-first-step-to-protect-against-it-hacking/) **is to be prepared for an attack from multiple vectors and assailants.** The notion that a hacker is a disgruntled youth in a basement may have origins in truth; however, it is far more likely that attacks are sophisticated, coordinated, and orchestrated by criminal organizations, or foreign states in addition to the motivated criminal individual. With most networks possessing multiple unsecured entry points, a proliferation of cloud-based services, and multiple connected devices inherent to the reality of conducting business in the healthcare industry makes for an increased "attack surface," where a single vulnerability invites an attack.

Mapping this attack surface (/blog/attack-surfaces-and-third-party-remote-access/) **and notating all points of entry and high-risk points can make it easier to continually assess, reassess, and reveal weaknesses.** Mapping offers an opportunity to take a close look at how healthcare data is accessed on your network. You're likely to discover that many access points (e.g. remote desktop, messaging applications, or VPN (/blog/the-risks-of-vpns-and-desktop-sharing-tools-for-remote-access/)) are ad-hoc and not designed for the level of usage their deployment often demands. **The goal here is to make your business a harder target.** Most healthcare data breaches are opportunistic in nature. Employing rigid standards of security and reinforcing your access portals goes a long way to closing down dangerous opportunities without sacrificing business-necessary access, like a nurse or healthcare professional whose access can't (and shouldn't) be restricted.

Monitoring EMR access shouldn't be a daunting task. Use this EMR Access Monitoring Checklist (/checklist/emr-access-monitoring-checklist/) to help build a successful access review process and eliminate the vulnerabilities that can threaten patient privacy.

(http://www.linkedin.com/shareArticle?mini=true&url=https://www.securelink.com/blog/healthcare-data-new-prize-hackers/&title=Hackers, breaches, and the value of healthcare data)

(mailto:?subject=Hackers, breaches, and the value of healthcare data&body=Check this out: https://www.securelink.com/blog/healthcare-data-new-prize-hackers/)

← PREVIOUS POST (HTTPS://WWW.SECURELINK.COM/BLOG/WHAT-IS-ZERO-TRUST-ARCHITECTURE/)

NEXT POST → (HTTPS://WWW.SECURELINK.COM/BLOG/WHY-PARTNERS-SHOULD-CONSIDER-ZERO-TRUST-NETWORK-ACCESS/)

(HTTPS://WWW.FACEBOOK.COM/SECURELINKINC)