Enhancing Cybersecurity in Texas Healthcare:

How to Prepare Against Cyber Threats

TEXAS HOSPITAL ASSOCIATION ENDORSED PARTNER

ActZero
actzero.com

OVERVIEW

Healthcare modernization revolves around data. Data fuels new diagnostics for patients, software for doctors, AI research to improve patient outcomes, and efficient business operations.

But this data is valuable to cyber criminals who are stealing it directly from hospitals, now more than ever. Breaches to hack into patient data or disrupt operations are increasing not only across Texas but throughout the entire U.S. healthcare system.[1]

Unfortunately for many hospitals, securing that data is a costly challenge. Ransomware attacks, laptop malware, email phishing, zero-day attacks, insider threats — it's difficult to keep up with cyber attackers 24/7 with limited IT budgets.

Reacting isn't enough, as a single ransomware attack can cripple your organization.

As the industry moves to introduce mobile devices for telehealth or remote patient monitoring, IT teams move their data to the cloud to support new infrastructure and tools. Data Centers hosting these critical applications and cloud products from Microsoft or Google remain vulnerable to extortion and disruption from ransomware, data theft, and social engineering.

Limited funds are always a challenge, and even when hospitals invest in cybersecurity, it's often a piecemeal approach with disconnected applications and solutions.

> "If you build software you are shipping a target, if you host software you are the target."
>
> —Brian Krebs, Security Researcher CISA.

[1] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

WHAT IS CONSIDERED A TARGET?

According to the FBI's Internet Crime Complaint Center (IC3), the FBI received more reports of ransomware attacks targeting the healthcare and public health sector than any other critical infrastructure sector in 2022.

Hosted Software

Many healthcare organizations rely on IT-enabled systems to store, process or transmit the health information required for daily work. These systems inherently provide more risks in protection and recovery to healthcare organizations directly because of the responsibility to build, deploy, and manage all aspects of the applications such as EPIC or other internally hosted electronic health records (EHR) applications. The more mission critical and the longer the rebuild the more attractive the target to disrupt as an attacker.

The more mission critical and the longer the rebuild the more attractive the target to disrupt as an attacker.

Smaller Organizations

Looking at wider trends, the demographics for targets tend to favor smaller organizations with fewer tools, processes, or IT personnel to monitor or recover from the events. In fact, 82% of ransomware attacks focus on organizations with less than 1000 employees.[2]

[2] https://www.strongdm.com/blog/small-business-cyber-security-statistics#:~:text=82%25%20of%20ransomware%20attacks%20in,had%20fewer%20than%20100%20employees

Time spent attacking these small organizations maximizes the opportunity for ransomware or extortion payments and wire-fraud. Of the 18 million U.S. businesses, roughly 15 million are less than 90 employees while the companies with between 100-1000 employees are 147,000.[3] Firms of this size are typically less likely to have dedicated IT security staff and who work with higher order law enforcement such as the FBI IC3 or Secret Service.[4] Maximizing the chances of wire fraud, crypto currency exchanges to succeed in extortion.

Outside Normal Business Hours

Hackers work outside the normal 9 am to 5 pm. In fact, 76% of ransomware attacks occur off-hours or on weekends.[5] This provides a window of opportunity to attack when team members are away, and it ensures those systems offline or disconnected from the network can be infected quickly upon return. With attackers only requiring 84 minutes on average to spread the initial infection to other systems across the data center, the ideal time to attack is the late evening prior to a holiday weekend return.[6]

$21 BILLION

More than 600 clinics, hospitals, and organizations in the U.S. were hit by ransomware in 2020 alone, accounting for more than 18 million patient records and an estimated cost of about $21 billion.

22.6 MILLION

Healthcare breaches affected more than 22.6 million total patients in 2021.

60% ATTACKS

Of all ransomware attacks, 60% specifically target healthcare and small and mid-sized hospitals are hit the hardest.

[3] https://www.naics.com/business-lists/counts-by-company-size/

[4] https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics#:~:text=If%20you%20are%20the%20victim,Report%20can%20be%20found%20online.

[5] https://www.zdnet.com/article/most-ransomware-attacks-take-place-during-the-night-or-the-weekend/

[6] https://www.crowdstrike.com/blog/crowdstrike-discusses-breakout-time-in-an-article-on-dark-reading/

WHERE ARE THE GAPS IN YOUR ORGANIZATION?

Insufficient Security Operations

Organizations may have some security tools in place, like antivirus or an EDR, to protect endpoints. Typically, IT directors add new tools to their technology stack over time, and while each investment addresses a new operational challenge, this piecemeal approach snowballs into a burden of alerts and tools that require tuning to protect.

Slow Patching, Poor configuration

Vendor released patches are one of the most common ways for an attacker to manipulate systems. Most organizations do not deploy patches automatically nor do they implement best practice configurations to systems. Remaining consistent and prioritizing this work within IT is an essential and often overlooked or easily forgotten aspect of day to day work.

> The more mission critical and the longer the rebuild the more attractive the target to disrupt as an attacker.

Identity Protections

Identity is the barbed-wired defense that protects your organization's assets by requesting credentials to verify identity for authorized access. The basic username and password authentication is inadequate for the brute force attacks executed by malicious actors. Furthermore, username and password combinations are easily procured by malicious actors on the dark web. Stealing digital identities is the most consistent and easiest way to access systems. While external systems such as VPNs and Email have traditionally been the entry points for attackers, there are many systems internally which do not deploy these protections. Administrative accounts tend to re-use the

usernames and passwords or provide rights automatically to newly created administrators. This allows attackers to maintain access in the organization, disable defenses typically without teams receiving notice.

Ability to Monitor and Respond During Off-Hours

Since bad actors attack when most staff are not working, organizations need to be confident their security teams can detect and respond to attacks anytime of day or night, specifically during off-hours or weekends. By 2025, 50% of organizations will use a version of remote threat disruption to help protect against threats. However, this number is only around 25% today.

Cost and Complexity

With licensing, staffing, implementation and monitoring costs of cybersecurity rising many organizations find difficult trade-offs in protection. Key systems such as anti-malware products are amortized and are not capable of detecting current state attacks. Other key systems such as firewalls or cloud products are not logging activity centrally or monitored by external teams.

Top Healthcare Breaches of 2022-2023

OneTouchPoint

Patients impacted: 4.11 million

Type of attack: Ransomware; Attacker accessed several servers one day before deploying the ransomware payload.

Other organizations affected: Anthem Affiliated Covered Entities, Blue Cross Blue Shield of Arizona, Blue Cross Blue Shield of Massachusetts, Clover Health, Geisinger, UPMC Health Plan

HCA Healthcare

Patients impacted: 11 million

Type of attack: data stolen from an "external storage location"

Other organizations affected: 182 hospitals and 2,220 care centers in 21 states.

EYE CARE LEADERS

Patients impacted: 3.6 million

Type of attack: Ransomware

Other organizations affected: 40 eye care providers

Patients impacted: 2.2 million

Type of attack: Ransomware

Other organizations affected: 119 provider offices

Shields HEALTH CARE GROUP

Patients impacted: 2 million

Type of attack: Ransomware

Other organizations affected: 60 healthcare providers

HAVE YOU BEEN HACKED? WHAT TO DO.

With the surge in healthcare organization cyberattacks, how do you know if you've been breached?

With the sophistication of modern attacks, sometimes it can take months to find out. On average organizations take more than half a year to detect a breach. There are a few telltale signs to suggest your data has already been compromised.

Clues that you've already been breached

Hackers don't announce their presence. The longer they remain hidden on your network, spreading and reconnoitering as they go, the more sensitive data they can scoop up, or damage they can do when they release their payload.

They naturally try to cover their tracks, but there are a few telltale signs you can look for:

Sudden file changes — Unfamiliar software unexpectedly installing, file name changes or other file tampering are signs you've been breached.

Locked user accounts — Users locked out of their accounts, and not because of numerous password attempts,, can mean others have been trying to access them or, worse, that a hacker already has access to the credentials.

Slow device and network performance — Systems compromised by botnet attacks or which have had processing power being harnessed for illicit purposes will slow down.

Antivirus "alerts" — Fake pop-up notifications that are hard (at least, for end users) to distinguish from the real system alerts.

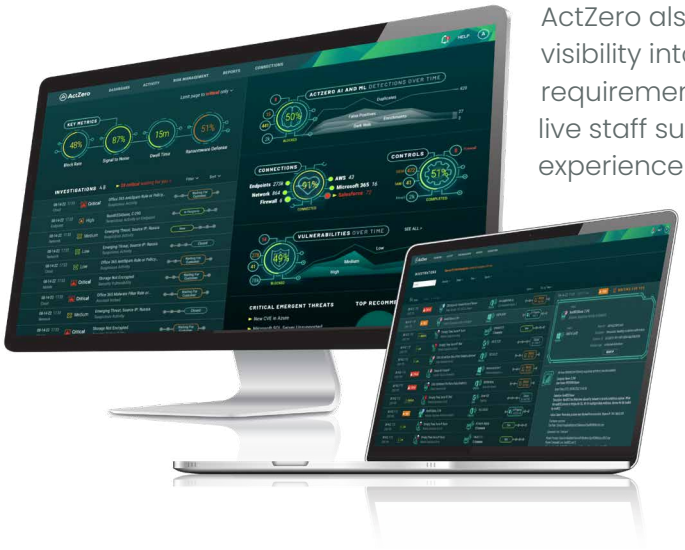
External sources — Partners or outside organizations inform you of a breach. By the time this happens, you've been breached for many months.

System alerts — Existing security solutions may be providing alerts. It's important to pay attention to these real alerts, although it can be difficult to separate what's real from the noise.

A PRESCRIPTION FOR HEALTHCARE CYBERSECURITY

ActZero, endorsed by the Texas Hospital Association, delivers a powerful and affordable full-stack cybersecurity service to protect hospitals against ransomware attacks. We bring deep expertise – from the White House, CIA, and Department of Defense – to you. We track the latest techniques of sophisticated cyber attackers and stop them quickly. Our proprietary AI enables us to stop threats four times faster than traditional defenses, uncovering advanced cyberattacks missed by most security solutions. We've automated most of the manual work to stop threats across endpoints, mobile devices, network, email, cloud, and identity systems within 15 minutes. Combining this AI with our 24/7 Security Operations Center staff expertise, we block fast-moving ransomware attacks, continuously filter out false positives and white noise, perform threat hunting daily, and escalate only critical alerts.

> "We've been pleased with ActZero from the initial sales meeting to implementation. Our relationship with them as a partner has never wavered, and we value them as an extension of our IT team. We receive quick responses and real-world help when we have a cybersecurity question. They have jumped at every request and always follow up with great customer service."
>
> —Mike Russell, CIO, Shannon Medical Center



ActZero also gives hospitals complete visibility into vulnerabilities, compliance requirements, executive reporting, and live staff support 24/7 from our customer experience team. This is a complete package to take care of cyberdefense requirements, meet compliance rules, qualify for cyber insurance, and keep your hospital safe.

TEXAS HOSPITAL ASSOCIATION ENDORSED PARTNER

ActZero

San Francisco / Seattle / Toronto / Dublin / Manila
info@actzero.com
actzero.com
+1-855-917-4981