ActZero

MODERN CYBERSECURITY FOR HEALTHCARE

CONTRIBUTORS

Adam Mansour
Chief Security Officer

Emily Bertrand
Sr. Director,
Strategy & Optimization

INTRODUCTION

IN HEALTHCARE DATA IS GOLD.

As healthcare providers continue to transform and look for new ways to address the growing need for their services and limited resources, data is the key. Through it, they can develop new digital tools, investigate ways to enhance patient outcomes, and improve business operations and processes.

Take, for example, electronic health records (EHR) and its promise of improving communications between practitioners and institutions, streamlining insurance processes, aiding in the move to self-directed care, reducing fraud and substance abuse — the list goes on. At the same time, having all that patient information stored digitally introduces new privacy concerns some aren't ready for.

THE GROWING NEED FOR HEALTHCARE TRANSFORMATION

The combination of an aging population and a rise in chronic illness is fueling the need for healthcare practitioners to find new ways to operate lean, while improving patient care, privacy and compliance.

Despite these pressures, some healthcare organizations have remained slow to digitize based on competing priorities, only exacerbating cybersecurity issues. Healthcare providers must find a special balance when it comes to their data. It's extremely sensitive and highly regulated so must be protected, but at the same time it must be able to be easily accessible to physicians, nurses, health scientists and others to improve care.

HEALTHCARE'S SECURITY CHALLENGES

For many providers securing that data can feel like a problem of epic proportions. Ransomware, malware, phishing, zero-day attacks, insider threats — there seems no end to what healthcare providers must contend with. As providers try to take greater advantage of their data, they must move to the cloud where there is the cost-effective infrastructure needed and automated tools to support the analytics needed to improve patient care. But does the cloud introduce new security risks? It's hard to even know where to start.

Meanwhile, where to invest the limited healthcare funds is always a challenge. It's not uncommon for cybersecurity to draw the short shrift when up against tools seen as more directly related to patient outcomes. Is it time to invest in better data protection, or a new MRI? Even when cybersecurity is invested in, it's often a piecemeal approach that results in a misunderstanding of the actual security posture of the healthcare organization.

To add to the challenge, finding great, expert cybersecurity talent today seems harder than brain surgery. Those organizations with existing cybersecurity expertise must closely guard against them becoming burned out due to being overwhelmed with low-value activities, or leaving for greener pastures as part of The Great Resignation, or Big Quit, of 2021 and 2022.

You need to protect the data entrusted to your organization, compliances like HIPAA require it, but how? It starts by understanding the adversary and what they're after.

The cybersecurity skills crisis has gone from "bad to worse," impacting more than half (57%) of organizations, according to a 2021 study by Information Systems Security Association (ISSA) and industry analyst firm Enterprise Strategy Group (ESG) — the fifth in a row illustrating this downward trend.

WHY HEALTH DATA?

As valuable as healthcare data is to healthcare organizations, it also is for bad actors.

Hackers are seeking either to disrupt your business or steal your incredibly valuable electronic protected health information (ePHI). When a hacker steals a credit card, online payment information or social security number they are getting only that. Steal healthcare information and they've hit the jackpot — a wealth of personally identifiable information, much of which can't be easily changed, dubbed "fullz" on the darkweb (where you will find around 140 million patient records up for grabs).

This makes healthcare information remarkably valuable on the darkweb and places where such illicit trading occurs. While a credit card number with its CVV is valued at around $5 on the darkweb, complete health records can go for up to $1000.

Of course, once hackers have access to your data, there's another reliable way for them to make money off their illicit efforts: ransom it back to you.

THE RISE OF RANSOMWARE IN HEALTHCARE

Ransomware is seeing a dramatic rise in the healthcare industry. In fact, they nearly doubled between 2020 and 2021 — with almost two-thirds of healthcare organizations hit by them. In fact, you can learn more about the PFS healthcare breach here and more about Quantum Locker Ransomware here.

With their eye on making money, ransomware has become one of the leading tactics of hackers attacking healthcare. Healthcare organizations are recognizing this growing threat and paying handsomely for cyber insurance in the hopes they can reduce the financial risks. Not only are cyber insurance rates skyrocketing, but to even be insured organizations must often prove they have certain security capabilities.

HACKER'S HEALTHCARE TARGETING TACTICS

- Through the wide network of third parties and users that providers must work with, from insurers to lawyers to other healthcare organizations — all of which may themselves be vulnerable.
- Through phishing attacks, sending malicious code in emails that unsuspecting users open and release onto the network.
- Stealing (or buying stolen) user credentials for another site or service and using them to access the network. Too many employees use the same password for services that become breached as for their corporate identity.
- Finding unsecured third-party access points from which to launch an unexpected attack.

A hospital can't generally afford to have any period when it can't access its records or may even face operational disruptions forcing them to reroute patients elsewhere — as in one tragic German incident — so threats of downtime are particularly effective.

What's insidious about ransomware attacks on healthcare organizations is that if you choose not to pay to access your data, you may still be extorted with the risk of it being released to the public. And what's worse, if you do pay the ransom, there's no guarantee that you'll get your data back, nor that it hasn't already been copied and sold. These are criminals, after all.

BY THE NUMBERS: HEALTHCARE CYBERSECURITY

$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.[1]

26.6 MILLION

Healthcare breaches affected more than 22.6 million total patients in 2021.[2]

60%

Of all ransomware attacks, 60% specifically target healthcare[3] and small and mid-sized hospitals are hit the hardest.[4]

HAVE YOU BEEN HACKED? WHAT TO DO.

With the surge in cyberattacks healthcare organizations are now facing — and the lucrative cash cow they promise to be for criminals — how do you know if you've been breached?

With the sophistication of modern attacks, it can take months to find out if you've had a breach. In fact, the average organization takes more than half a year before they detect a breach. Still, there are a few telltale signs your data might already be compromised.

LOOK FOR:

- **Sudden file changes**
- **Locked user accounts**
- **Slow device and network performance**
- **An alert from your system**

While it can take months before a breach is detected, you can always enlist the help of a professional to do an assessment.

Incident Response Steps

IR Steps	Supporting Resources	Download
Identify – Who is impacted, which devices, what processes?	To see how, check our our IR Guide	
Contain – Eliminate suspicious activity, kill the processes, delete files or block the user.	For methods, see our Foundations of IR Readiness ebook	
Analyze – Once contained, find out what happened and how the hacker gained entry.	Watch our panel discussion Thinking About the Adversary: Offensive & Defensive Strategies for things to look for.	
Prevent – Stop the attack from spreading through your network or getting in again.	See the Access Control steps in our CMMC Controls Mapping	
Remediate – Patch to address vulnerabilities; prioritize based on the type of breach.	For high-profile zero-days, guidance is often issued from the vulnerable developer — here's an example of our coverage on log4shell.	
Recover – Gain control. If hit with ransomware this may mean reverting to a backup.	Recovery is going to be specific to each organization's disaster recovery (DR) strategy. Read Evaluating Paths to IR to see some of the challenges with backups.	
Communicate – Inform users, management and appropriate regulatory bodies.	To disclose compromised patient information, use the HHS website. To disclose other compromised information (like PII, such as credit cards paired with addresses), there are state-specific bodies to notify. See our Breach Notification Rolodex, at the end of the IR Guide.	
Debrief – What have you learned? Create a plan to address areas needing improvement.	Find detailed instructions in our blog, Tenets of IR Postmortem (RCA)	

If you don't have in-house expertise, you might need to seek help for one or more of those steps.

IMPROVING YOUR SECURITY POSTURE. WHERE TO START.

There's a lot of hype in the cybersecurity industry, and the threat landscape is constantly changing. What should healthcare organizations prioritize to build a more proactively preventative security posture?

There's no one-size-fits-all answer. But here are four things to consider, depending on how far along you are on your cybersecurity journey. Some of these steps you can begin on your own, others you will likely need help with. Whether you have the resources internally, or seek outside assistance, working with a professional is crucial.

Steps to build cyber security

1	**Ransomware Readiness Assessment** - Have (or perform) a professional audit of your current security posture, including testing of your defensive capabilities using darkweb-sourced malware simulations, and an attack-intent assessment. It should inform you of lost or stolen health information already on the darkweb, as well as learning what passwords and accounts are compromised.	 **Start Free Assessment**
2	**Threat modeling** – Determine which elements of your network and systems need to be protected, and which are at risk. Get a more complete understanding of your security posture. There are several threat modeling techniques that can be used. ActZero follows a simple, highly effective three-step process: assessment, analysis and mitigation. First you identify the threats or vulnerabilities, then analyze why and how they are happening, then take the actionable steps to prevent them in a prioritized fashion: start with your highest-level threats. Work with your security experts to understand and protect from the greatest threats and areas most at risk and expand your security activity from there. Use what you gleaned from your threat modeling and apply threat intelligence and threat mapping to address the problems. This is a place many organizations need outside assistance.	 **Read Blog**
3	**Always-on security** – The adversaries today are relentless, and any security strategy must account for that. Consider using AI as the first line of defense — it never sleeps, after all — followed by professional threat hunters as a second one. Place intelligent agents on your computers, mobile devices, servers and other endpoints to continuously and autonomously monitor activity and report it to threat hunters or AI that detect suspicious behavior. Leverage the best of both machine and human intelligence to do what they each do best.	 **Visit Website**
4	**Compliance, compliance, compliance** – Because of the highly sensitive nature of healthcare information, every strategy around data use and its protection must be in compliance with NIST, an internationally recognized framework, and the HIPPA Security Rule. Make sure you have all aspects covered to gain compliance; however, working with a professional can help streamline this regulatory process and ensure you've covered everything.	 **Download**

A PRESCRIPTION FOR HEALTHCARE CYBERSECURITY

Today, healthcare data is as valuable to your organization as those who threaten it with cyberattacks.

You need that data to improve the business, provide better patient experiences and improve health outcomes; they want it because it's lucrative on the black market. You can't lock it down from the people who need it to spark change, but you are obligated to protect it from cybercriminals and the public.

There are a lot of buzzwords in the industry, and the cybersecurity landscape seems to change faster than most can keep up with. You need to look past the noise and hype and stay focused on understanding the threats to your organization and how to proactively prevent them.

Working with specialists like ActZero is a great first step in your work towards keeping a continuous, vigilant eye on the health of your network, endpoints and systems security—but even more, it can provide immediate innoculation against the ransomware that puts your organization and patients at risk.

Give us an hour to prove it, you may find we're just what the doctor ordered.

info@actzero.ai | +1.855.917.4981

ActZero

TORONTO
5045 South Service Road, Suite 300
Burlington, Ontario
L7L 5Y7

MENLO PARK
2882 Sand Hill Road, Suite 115
Menlo Park, California
94025

SEATTLE
Hawk Tower
255 South King Street, Suite 800
Seattle, Washington
98104