How to Raise Your Organization's Game to Combat Cybercriminals

As cybersecurity threats to health care organizations escalate, your responsibility as a senior hospital or health system leader is implementing high-level detection and remediation solutions.

AVERTIUM® | LogRhythm® | American Hospital Association™ Advancing Health in America

The average attack recovery expense, including downtime, manhours, device cost, network cost, lost opportunity and the ransom paid, was nearly $1.3 million

The numbers should make senior hospital and health system executives lie awake at night.

Through the first six months of 2021 alone, health care providers reported more than 250 data breaches of protected health information (PHI) to the HHS Office for Civil Rights. One hundred of the reported breaches involved cybercriminals hacking into the network servers of provider organizations.

In fact, 34% of more than 300 health care organizations recently surveyed by Sophos, a business cybersecurity firm, said they were hit by a ransomware attack over the past year. The average attack recovery expense, including downtime, manhours, device cost, network cost, lost opportunity and the ransom paid, was nearly $1.3 million.

Experts interviewed for this white paper on cybersecurity say it's not a matter of if bad actors will attack, it's a matter of when. With cyberattacks, nothing is off limits. The combination of immensely valuable data, the potential to cause harm to a vast number of people and the lack of investment in cybersecurity investments makes health care an enticing target. Given the escalating threat, experts say hospitals and health systems like yours must elevate their games to protect their operations and, more importantly, their patients from cybercriminals.

This white paper identifies the reasons why hospitals and health systems have become a favorite target of cybercriminals and offers practical, albeit sophisticated, strategies and tactics that you as a leader can implement to successfully prevent and mitigate cyberattacks.

It's time to build a better cybersecurity strategy.

AVERTIUM | LogRhythm | American Hospital Association™ Advancing Health in America

Why Hospitals and Health Systems?

When cybercriminals attack your hospital or health system and steal or hold your PHI for ransom, the first question you ask as a senior leader is, "Why us?" as if the attack were a coincidence or stroke of bad luck. Coincidence and luck have nothing to do with why bad actors chose you. They picked you specifically and deliberately because of who you are, what you have and how you operate.

Let's run down a few of the primary reasons for cybersecurity attacks:

The data you have. The data you have in the form of PHI is uniquely valuable to cybercriminals. Unlike other types of data that can be canceled and replaced like a credit card number or a phone number, PHI has enduring value. There is only one of you, and your health records can't be canceled and replaced. Not only does PHI have enduring value, but it also comes with a rich data set. That data set includes dates of birth, Social Security numbers, home addresses, health insurance policies, credit card numbers, bank accounts and more — not just from the patient, but also from the patient's family. PHI is exponentially more valuable than other types of data.

The data you share. As you know, health care is one of the most, if not the most, regulated fields in the country. Complying with rules, regulations and standards means that you're sharing your PHI with a seemingly endless list of public and private organizations. You're continuously transmitting your PHI via your information technology (IT) systems to state and federal government agencies, commercial

Three examples of recent cybersecurity attacks on hospitals and health systems

1 A suspected ransomware attack shut down the health IT systems for weeks at more than 400 facilities operated nationwide by an investor-owned hospital chain with a reported recovery expense of $67 million.

2 A ransomware attack placed malware on more than 5,000 computers and laptops that locked files and data on 1,300 servers at a nonprofit health system in the Northeast with a reported recovery expense of $64 million.

3 A ransomware attack on a nonprofit hospital in the Midwest forced the hospital to shut down its entire computer network and divert ambulances for nearly a week, restricting care to only walk-in emergency patients and pregnant women in labor.

health plans, accrediting bodies and more. Every piece of technology that you use and every time you use it to transmit PHI for compliance purposes, you expose your yourself to a potential cybersecurity attack.

Your "attack surface." Your hospital or health system shares a lot of data, but whatever volume of data you share, you likely take in or accept even more. Collectively, each data intake point — from your online scheduling system to your electronic health record (EHR) system, remote patient monitoring devices or a telemedicine visit to a supply chain ordering form — is called your attack surface by cybersecurity experts. It's the totality of the technology front that you must defend against cybercriminals. It's vast, and the COVID-19 pandemic made it even bigger with the rapid expansion of virtual care models and work-from-home options.

Your caring culture. Both what you do and why make your hospital or health system especially vulnerable to cybersecurity attacks. First, the people who work for you — from front-line caregiver to back-office business staff — are caring by nature. They want to help people, and that makes them more trusting of anyone who needs something, like a cybercriminal posing as a concerned patient in an email. Cybercriminals know what's at stake if they can steal or freeze your PHI. Any delay or disruption in care puts patients' health and lives at risk regardless of whether you're a Level I trauma center or a sole community hospital. That makes you more likely to pay perpetrators quickly to get back access to your data.

When you consider those four primary reasons, you may think there's not much your hospital or health system can do beyond what it's doing already to prevent and managed cybersecurity attacks. But there is, and the time to act is now.

AVERTIUM | LogRhythm | American Hospital Association™ Advancing Health in America

The American Hospital Association thanks the following cybersecurity experts for their input and insights that informed this white paper.

Paul Caiazzo

Chief information security officer

Avertium

Phoenix

John Riggi

Senior adviser for cybersecurity and experience

American Hospital Association

Washington, DC

Scott Waters

Chief information officer

Overlake Medical Center & Clinics

Bellevue, Wash.

James Carder

Chief security officer and vice president

LogRhythm Labs

Boulder, Colo.

9 Ways to Elevate Your Cybersecurity Program

Health care cybersecurity experts recommend the following tactics and strategies to better protect your operations and your patients during this time of heightened cybersecurity risk. Think in terms of people, processes and technology.

People

1 Devote the appropriate resources to cybersecurity. Build a cybersecurity team commensurate with the cybersecurity risk facing your hospital or health system. Headed by your CIO or chief information security officer, your team should include senior security engineers, junior security professionals and, when needed, third-party security experts from managed-services providers.

2 Build an enterprisewide culture of cybersecurity. Maintaining the privacy and security of PHI must become as ingrained in your culture as providing superior patient care. Staff training must be ongoing and show how each person's actions create or minimize risk. Programs also should feature both rewards and sanctions.

3 Lead from the top with the C-suite and governing board. Hospitals and health systems with effective cybersecurity programs have one thing in common: Their senior executive team and governing board are fully engaged in maintaining the privacy and security of PHI. They fully recognize cybersecurity as an enterprisewide risk and responsibility.

Processes

4 Understand and manage your attack surface. If your attack surface is limitless, you have no chance to stop a cybersecurity attack. If you limit your attack surface, you can decrease your risk considerably. Inventory your tech-enabled data access points and then close or centralize them through a common network. Learn more about attack surface management.

5 Update and increase incident planning. You must take the same approach to cybersecurity as you do with other types of disaster planning. Once you detect a risk or a breach, you must know what to do immediately. Given the growing types and sophistication of attacks, regular scenario planning at least quarterly is critical. It doesn't do any good to have a plan and not know how to actually execute it.

6 Stay up to date on threat actors. As a senior executive, it's unrealistic to track new threat actors targeting your operations and do your day job. This is when third-party security experts can be sound additions to your cybersecurity team. Annual threat briefings can provide a view around the corner of what new tactics threat actors are deploying. Learn more about the latest threat actors.

Technology

7 Update your monitoring, prevention and reporting technology. Outdated technology can breed chaos and invite trouble. Cybersecurity detection, prevention, and monitoring and reporting systems must be updated for the latest threats and be flexible and scalable as your hospital or health system expands virtual care options for patients and its attack surface. Beyond proper cybersecurity hygiene, multi-factor authentication, and employee

education, it's imperative to have visibility into the assets at risk and the correct security controls in place to protect those assets.

8 Use multifactor authentication to access all systems. It shouldn't be harder to get into your phone than it is to get into your EHR. Your cybersecurity program must require multifactor authentication by all users across your entire attack surface. That also means updating and testing it regularly.

9 Build and monitor meaningful cybersecurity KPIs. The first step in creating meaningful key performance indicators for your hospital or health system is baselining your cybersecurity risks. How many phishing threats do you get each day? How much malware do you regularly block? Your technology should monitor and flag suspect deviations in those baselines.

Conclusion

The cybersecurity risks challenging your hospital or health system are going to become more frequent, more intense, more sophisticated and more costly. Like mice on steroids, they'll overwhelm and overrun your operations and threaten the care that you provide to your patients. Your best and only option is to modernize your prevention, detection and mitigation program.

It's time to build and exercise on a regular basis a better cybersecurity defense plan.

Resources

- HHS Office for Civil Rights Breach Portal
- The State of Ransomware in Healthcare 2021, Sophos, May 2021
- Health Care Industry Cybersecurity Task Force Resource Catalog
- Health Industry Cybersecurity Supply Chain Risk Management Guide (HIC-SCRiM)
- Health Industry Cybersecurity Protection of Innovation Capital (HIC-PIC)
- Medical Device and Health IT Joint Security Plan
- Joint Cybersecurity Advisory - Ransomware Activity Targeting the Healthcare and Public Health Sector
- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients
- FBI – Ransomware
- HIPAA Compliance and Beyond

American Hospital Association™

Advancing Health in America

The American Hospital Association (AHA) is the national organization that represents and serves all types of hospitals, health care networks, and their patients and communities. Nearly 5,000 hospitals, health care systems, networks, other providers of care and 43,000 individual members come together to form the AHA. Through our representation and advocacy activities, AHA ensures that members' perspectives and needs are heard and addressed in national health policy development, legislative and regulatory debates, and judicial matters. Our advocacy efforts include the legislative and executive branches and include the legislative and regulatory arenas. Founded in 1898, the AHA provides education for health care leaders and is a source of information on health care issues and trends. **www.aha.org**

AVERTIUM®

Avertium is the managed security and consulting provider that companies turn to for end-to-end cybersecurity solutions that attack the chaos of the cybersecurity landscape with context. By fusing together human expertise and a business-first mindset with the right combination of technology and threat intelligence, Avertium delivers a more comprehensive, more programmatic approach to cybersecurity — one that drives action on the ground and influence in the boardroom. That's why over 1,200 midmarket and enterprise-level organizations across 15 industries turn to Avertium when they want to be more efficient, more effective and more resilient when waging today's cyberwar. Show no weakness. **www.avertium.com**

Click here to schedule your threat briefing now.

LogRhythm®

LogRhythm is a world leader in NextGen SIEM, empowering organizations on six continents to successfully reduce risk by rapidly detecting, responding to and neutralizing damaging cyberthreats. The LogRhythm platform combines user and entity behavior analytics (UEBA), network traffic and behavior analytics (NTBA) and security automation & orchestration (SAO) in a single end-to-end solution. LogRhythm's Threat Lifecycle Management (TLM) framework serves as the foundation for the AI-enabled Security Operations Center (SOC), helping customers measurably secure their cloud, physical and virtual infrastructures for both IT and OT environments. Built for security professionals by security professionals, the LogRhythm platform has won many **accolades**, including being positioned as a Leader in Gartner's SIEM Magic Quadrant for 9 consecutive years.