CyberMaxx

The State of Cybersecurity in Healthcare

How increased vulnerabilities from emerging medical delivery models and changing consumer demands impact data security and patient care

Executive Summary

As healthcare technology evolves to make medical information more accessible to physicians and patients, bad actors exploit these conveniences to infiltrate healthcare institutions.

Healthcare cyberattacks are becoming more common. In Q1 2023, the healthcare sector experienced an average of 1,684 attacks per week, according to Check Point Research. This data represents a year-on-year increase of 22%.

These attacks are also becoming more expensive. According to IBM's X-Force Threat Intelligence Report, the average costs of a studied breach in healthcare reached nearly $11 million in 2023.

There's a good reason why healthcare is one of the biggest targets for bad actors. Confidential patient information and medical records are worth a lot of money, and attackers know they can use this as leverage to increase the pressure on organizations to pay the ransom.

As healthcare cybersecurity professionals, we must maximize our security posture while minimizing disruptions to ensure patients don't suffer the ramifications of healthcare IT vulnerabilities.

CyberMaxx investigated the current state of healthcare cybersecurity to uncover the most cutting-edge medical innovations and cybersecurity threats so you can be prepared to triage risks as effectively as possible.

Greatest Challenges Facing Healthcare Organizations Today

Healthcare is changing rapidly, and fewer patients are pursuing primary care. Almost 1-in-3 patients who received medical care between 2016 and 2022 did not see a primary care physician, according to a FAIR Health analysis published in March 2023.

The report also revealed that the number of people visiting retail health clinics increased by 51%, and those visiting urgent care centers increased by 14% between 2020 and 2021.

Many of these trends appear to be driven by the COVID-19 pandemic. Telehealth use has increased 38X from the pre-COVID-19 baseline, according to a McKinsey & Company study published in 2021.

This increased reliance on online specialists and on-demand healthcare compounds the need for electronic medical records to ensure patient safety and efficiency of care when receiving treatment from multiple physicians and institutions.

The Security Risk of Meeting These New Expectations

These changes are leading to an obvious new standard: digitizing healthcare delivery and on-demand access to health records.

Market demand for transparent, web-first healthcare information requires an unprecedented level of information-sharing. Patients want access to protected health information (PHI), like test results, on their personal devices.

While there's a huge push for smartphone apps containing PHI, ensuring consumer devices are secure presents many challenges.

Information sharing goes far beyond patient access to medical information. The industry's increased focus on specialists, telehealth solutions, and doc-in-a-box also suggests the need for personal information to be shareable with tertiary healthcare providers.

Each new user introduces the potential for a new security breach caused by human error, and the convenience offered to patients and medical professionals must be considered another door for potential cyber criminals.

The Security Risk of Meeting These New Expectations

"Let me tell you what several dozen of my healthcare industry victims [at the FBI] had in common: they were all HIPAA compliant," says Scott Augenbaum, a retired FBI agent who spent almost 25 years fighting cybercrime. "So what does that mean? Being compliant isn't the same thing as being secure."

The hardest part about implementing adequate cybersecurity controls in a hospital setting is that cybersecurity has traditionally been treated as a remediation to an audit or compliance requirement.

Hospitals don't bring in a cybersecurity solution because it makes their healthcare organizations earn more money, save more patient lives, or accomplish other business goals. Most healthcare organizations invest in cybersecurity for the same reason they buy fire insurance: to save their patients, business, and employees from disaster.

Patients don't just trust healthcare organizations with their lives – they also trust them with their data. Therefore, patient data safety should be a top priority.

Cyberattacks Can Have a Human Cost

Cybersecurity professionals must be aware of the impact of their work on clinical outcomes. The cost of failing to put adequate security protocols in place is high.

Security protocols added *after* a data breach in an attempt to restore data security can be associated with increased mortality rates for patients with critical conditions like a stroke or heart attack, according to one study published in Health Services Research in 2019.

When doctors complain to business executives about the increased keystrokes or time required to log in to patient records, the execs go to IT and InfoSec. As doctors and execs become frustrated, InfoSec can be viewed as the problem.

Saving Lives Through Increased Cybersecurity

Given that the stakes are so high, there's a strong demand for cybersecurity precautions that don't slow down medical professionals. "Security has to enable the everyday functions of a hospital, not block them. We have to strive to find controls that are effective but transparent," says Thomas Lewis, founder and current board member of CyberMaxx.

Unfortunately, many healthcare practitioners – the end users of these products – have been left out of the discussion. "Even the clinicians – the doctors and nurses – typically hate whatever electronic medical record (EMR) they're using. These EMR systems came about through HIPAA legislation, which was more of a requirement to facilitate data transfer. At the outset, they didn't take into account the way clinicians work," says Scales.

Implementing inefficient IT processes can negatively impact professionals across an entire healthcare organization. It can have both human and financial implications. It's InfoSec's job to analyze these implications. When doctors complain to business executives about the increased keystrokes or time required to log in to patient records, the execs go to IT and InfoSec. As doctors and execs become frustrated, InfoSec can be viewed as the problem.

IT can boost efficiencies across an entire organization when it's done strategically. IT efficiencies have the power to minimize operational costs and give doctors more flexibility and work-life balance. For example, doctors can sign off on charts from home.

"When we are fortunate enough to interact with clinicians and high-level execs at the companies we serve, our message is that we try to help them understand the overall cybersecurity problem so that they know how their day-to-day activities factor into cybersecurity outcomes. We try to speak their language," says Jason Riddle, former President and COO of CyberMaxx.

InfoSec must work to mitigate the operational impact of security controls and find more efficient innovations, like single sign-on, that simplify everyday processes for clinicians.

Medical Devices and IoT

The place where the Internet of Things (IoT) and healthcare intersect is still in its infancy. Industrial and consumer IoT products provide enormous convenience to end users, which has allowed the industry to grow rapidly. In the healthcare industry, there are two key parts of IoT that medical professionals may interact with regularly: smart medical devices and general consumer IoT.

"Smarter medical devices and robotics are increasing in usage within providers; these devices, when insecure, can greatly endanger patients and create great liability for providers," says Lewis.

56% of respondents said that their organizations experienced one or more cyberattacks in the past 24 months involving IoMT/IoT devices, according to a report published in 2022 by IT services company Cynerio and research organization the Ponemon Institute. The report resulted from surveying 517 healthcare experts in leadership positions at hospitals and healthcare systems throughout the United States.

Furthermore, 45% of these respondents reported adverse impacts on patient care from these attacks, and 53% percent of those (24% in total) reported adverse impacts that resulted in increased mortality rates.

Smart Medical Devices

What happens when an implanted biomedical device used to keep your body running gets hacked?

There are multiple biomedical devices running on smart technology. According to Healthline, pacemakers are among the most hackable devices. In 2020, a woman hacked her own pacemaker to show how vulnerable we are to cyberattacks. As the usage of potentially hackable biomedical devices continues to rise, patients, manufacturers, and medical institutions are increasingly at risk. And as technology becomes more sophisticated, so do cybercriminals.

Connected devices that feature remote monitoring and require constant updating and patching, like insulin pumps, defibrillators, and cardiac monitors, are some of the biggest targets for cyberattacks, according to a 2019 report by Moody's Investors Service.

Top medical device makers, including Abbott and Medtronic, have started to work in collaboration with white hat hackers and InfoSec researchers to secure medical devices. As part of this collaboration, they have even staged immersive hospital-based hacking scenarios at the Biohacking Village, a multi-day biotechnology conference designed to celebrate global health ingenuity.

Some key smart medical device security risks that must be addressed include:

- Biomed support is largely outsourced, and security responsibilities may not be clearly defined
- A lot of medical software runs on Windows. Many healthcare institutions will defer essential updates for years because the process is so low on their priority list. However, the potential cost can be high
- Medical devices often don't report through IT, so they don't follow IT's control processes
- Outdated medical devices present a clear security vulnerability, and dedicated systems are needed to quarantine and isolate them from the rest of the network if they can't be replaced with newer machinery
- Many medical devices store patient information. As these tools become dated, many healthcare institutions may simply throw them away without first deleting confidential patient data stored on the devices (such as printers, EKGs, or insulin pumps)

Consumer IoT Devices at Healthcare Institutions

The use of consumer devices in clinical environments presents ongoing challenges. Doctors might wonder why they can't have an Alexa in the office without considering the privacy issues these consumer devices present. For instance, cybercriminals can use consumer tech devices to hack into clinical settings and eavesdrop. In the worst case, they could even use them as a means to gain access to the hospital's IT network.

Though Amazon is entering the healthcare industry with the introduction of a new HIPAA-compliant Skills Kit, that doesn't mean that generic consumer smart speakers are HIPAA-compliant and appropriate for clinical settings.

In 2019, Amazon announced its entry into the healthcare industry by introducing a new HIPAA-compliant Skills Kit. However, this move has raised concerns among experts, who have criticized the move as "seemingly another move by the tech giant to know every last detail about your life" and pointed out Amazon's poor track record when protecting personal data.

It's also a well-established fact that Amazon employees are paid to listen to recordings from smart speakers. In addition, smart speakers have been known to send messages to third parties inadvertently.

In 2019, researchers from cybersecurity consultancy and research collective Security Research Labs (SRLabs) found that malware could easily be disguised as a seemingly harmless Alexa skill or Google action – third-party add-ons that some users install to add functionality to their smart speakers.

This would allow cybercriminals to secretly record dialogue or attempt to get the user's Google password through phishing. In a clinical setting, this is akin to inviting cybercriminals to be a fly on the exam room wall.

Growing Networks and Evolving Risks

Ransomware

Ransomware remains one of the biggest threats to the healthcare sector. According to the FBI's 2022 Internet Crime Complaint Center (IC3) report, the healthcare sector suffered more ransomware attacks than any other sector and at least twice as many as most others.

The FBI received 870 reports of ransomware attacks aimed at organizations belonging to 16 critical infrastructure sectors – 210 of these reports were in the healthcare sector.

In May 2017, the National Health Service in the UK was hit with a massive ransomware cryptoworm attack called WannaCry. At the time, there was no official cyberattack response plan in place. The largest impact of this attack was that an estimated 19,494 patient appointments were canceled – including scheduled patient operations.

Social Engineering Attacks

Social engineering attacks, including phishing, pretexting, and spear phishing, are other common threats. "Your last line of defense is your end users. If they click the wrong email, accept the wrong file, or store a password in an insecure location, then it's done. All that money I've spent and all the safeguards I have up are no good anymore." says Scales.

And it's not just the untrained clinical assistants that are at risk. Senior executives are twelve times more likely to be targeted in social engineering incidents, according to Verizon's 2019 Data Breach Investigations Report.

The Verizon report also found that 80% of hacking-related data breaches occur because of compromised passwords.

Weak or compromised passwords are yet another easy target for brute force attacks. Without additional security protocols like two-factor authentication, a stolen password can easily cascade into stolen personal or business information.

The Verizon report also found that 80% of hacking-related data breaches occur because of compromised passwords.

One of the most effective ways to protect your organization from so many potential user errors is by training your clinical staff and employees – including your C-suite employees – to notice suspicious activity and report it immediately while following protocols for setting safe passwords. You should also ensure employees understand why enabling two-factor authentication on their online accounts is important.

Securing Vast Interconnected Networks

Another potential security issue is the exponential number of entry points into the hospital network. "By nature, hospitals have always been difficult to secure," says Lewis. "Often, one of the biggest risks is that new systems and integrations to the network aren't tested and vetted by InfoSec. They're just implemented."

This is one of the main concerns with 5G technology. In major metro areas, back offices realized they could start to connect to biomedical devices or third-party imaging servers directly, sending PHI across an unsecured connection.

In September 2019, ProPublica revealed that millions of images on servers run by independent radiologists, medical imaging centers, and archiving services were accessible online – unprotected by even the most basic security precautions. Inevitably, integrating with third parties or outside servers means you can't quickly patch vulnerabilities. Hospital InfoSec must be able to take full responsibility for its own network and manage the risk posed by the vulnerabilities in outside systems.

Scales points out that third-party applications that integrate with EMRs are another risk. "With some of the smaller EMRs, clients tend to go out and partner with other third-party products who can fix particular operational and clinical problems," he says. "If that one third-party vendor gets compromised, then you can compromise your entire system. There are so many end-points now, it's incredibly difficult to keep cybercriminals out."

Integrating InfoSec into the purchasing and procurement process is critical to managing the sliding scale of risk regarding medical devices and outsourced services.

The Challenge of Big Data

Medical professionals are constantly creating data. Meanwhile, they're leveraging increasingly complex infrastructure to house this data.

Machine learning and artificial intelligence (AI/ML) are growing in importance when securing healthcare infrastructure. Managing such a large amount of data is only possible with help from algorithms that can track patterns, identify abnormalities, and detect malware so that InfoSec can quickly stop attacks and implement effective countermeasures.

Riddle points out that data analytics is helping us to quickly detect sophisticated attacks that would otherwise fly under the radar. "We're finding things now that we probably wouldn't have found five years ago because of the data analytics tools we have available today. And these tools are getting better every day," he says.

But as security professionals implement AI/ML, so do cybercriminals – and they can often act more quickly and efficiently than slow, bureaucratic healthcare institutions.

In early 2019, Israeli researchers showed that malicious actors could use deep learning to add or remove evidence of medical conditions from volumetric (3D) medical scans.

In a covert penetration test, they intercepted and altered CT scans at an active hospital. Researchers suspect this type of malware could be used to tamper with MRI and CT scans to commit insurance fraud, tampering with test results from high-profile individuals, or even commit sabotage or murder.

Rapid Activity in Clinical Acquisitions

In the first quarter of 2023, there were 15 healthcare industry transactions, a slight drop from 17 in the fourth quarter of 2022, according to a report from hospital consultancy Kaufman Hall. Transaction size and transacted revenue are both trending upward.

In acquisitions, the purchasing party often doesn't know the technological challenges they're walking into. There's no single EMR system used universally across healthcare networks. Many smaller healthcare organizations still use paper charts or do less to prioritize data safety than the acquiring organization. Without the right preparation, it's easy to purchase a patient-data disaster accidentally.

Dated, legacy systems are a growing problem in the healthcare industry, which is often slow to adopt new technology.

Multiple factors are causing the slow adoption of new technology. Some come down to price: it can cost thousands to multi-millions of dollars to install a robust, secure IT system with appropriate security controls, monitoring capabilities, and more.

In addition, smaller healthcare institutions – particularly those run by veteran healthcare practitioners – fear making huge changes to daily processes. It's hard to reset the daily working standards of an office, especially when some team members have used the same protocol and technology for decades. Unfortunately, using old, outdated technology that's no longer being updated can pose a significant security risk for organizations.

Budget Constraints

According to Moody's report, smaller hospital systems are most vulnerable to cyberattacks precisely because of their budget and talent restraints.

Due to the large upfront investment in adopting electronic medical records, younger practitioners are more inclined to use EMRs than doctors nearing retirement. This is because spending tens of thousands of dollars to update systems in their final years of medical practice is unappealing. Many are opting to maintain physical records for their immediate convenience.

Upcoming medical students are being prepared to use and handle electronic records in medical school. Paper charts are almost obsolete to the millennials and Gen Zs currently coming up through medical school.

At the same time, retiring doctors are handing off decades of patient medical data to be transferred to electronic format. To meet compliance, some of these paper records are being stored for years in doctors' homes and offices.

Preparing the Next Generation of Medical Professionals for Cybercrimes

Protecting patient medical data has always been an important element of the medical profession. As these records have become increasingly digitized, new threats emerge.

At Vanderbilt University, nursing students are given a robust IT orientation. They're taught some of the most common ways cybercriminals access patient medical information, including social engineering attacks.

Dr. Geri Reeves says, "We have a pretty sophisticated student orientation with our IT dept. They are detailed on the importance of keeping patient information safe – that's the verbal record, written record, and electronic health record."

There's still a wide discrepancy in technological adoption between large corporate-owned hospital chains and small, independently-owned medical practices. A discrepancy also exists between for-profit and non-profit systems. Healthcare, as an industry, is still evolving and will continue to evolve for years to come.

Acknowledgments

We would like to thank the following experts for their unique contributions to this whitepaper:

- Scott E. Augenbaum, MBA, author of *The Secret to Cybersecurity: A Simple Plan to Protect Your Family and Business from Cybercrime*
- Geri Reeves, Ph.D., APRN, FNP-BC, Associate Professor of Nursing at Vanderbilt University
- James Botsko, MD, Family Medicine Doctor
- Joshua Scales, CLSSGB

About CyberMaxx

CyberMaxx, LLC, founded in 2002, is a tech-enabled cybersecurity service provider headquartered in New York, NY. Through a comprehensive set of services CyberMaxx empowers customers to Assess, Monitor, and Manage cyber risk and stay ahead of emerging threats. CyberMaxx expanded its capabilities through the 2022 acquisition of CipherTechs, an international cybersecurity company providing a complete cybersecurity portfolio across MDR Services, Offensive Security, Governance, Risk & Compliance, DFIR, and 3rd-party security product sourcing.

CyberMaxx's managed detection and response solution (MAXX MDR) is designed to be scalable for clients of all sizes, providing protection and improving the organization's security posture, ultimately giving customers peace of mind that their systems and data are secure.

Learn More, Today!

To learn more about CyberMaxx's solutions please visit, CYBERMAXX.COM to get started.