Critical Insight

American Hospital Association

5 Cyber Problems That Healthcare Can't Ignore

Expert Insights from John Riggi and Drex DeFord

Table of Contents

Introduction

It's a sad reflection on the state of the world, but as COVID-19 has stretched healthcare providers across the country, malicious actors have looked to exploit the crisis for their own ends. Healthcare has always been a prime target for cybercriminals. Successful attacks leading to data breaches that contain sensitive and personal patient information net attackers the highest price when sold on the dark and deep web.

This is due to the nature of the information held in medical systems and records: names, addresses, social security numbers, Medicaid ID numbers, health insurance information, and medical histories. As early as February 2017, Accenture reported that 26% of Americans had been the victims of healthcare information data breaches. The frequency and sophistication of attacks have only increased in the intervening years.

Protecting healthcare systems and information from attackers is therefore crucial. But the threat landscape that healthcare providers face is wide, ever-changing, and an area that requires specialists to counter adequately. Clearly, this is now an area of business that all healthcare providers need to ensure is covered and that they have cyber-protections in place.

“Healthcare providers face a threat landscape that is wide and ever-changing”

It is also not in the core area of expertise for most healthcare organizations who will need to engage with external cyber security experts. In this white paper two experts in the field, from differing but highly complementary backgrounds, outline five cyber security vulnerability areas that healthcare providers need to address.

Authors

Together John and Drex have the knowledge, experience, and cybersecurity industry contacts that healthcare providers will need to safeguard their IT and patient care systems from cyberattacks.

The five topic areas they discuss, and many others, are among the issues the team at Critical Insight help healthcare organizations solve. Critical Insight extends your team by providing a mix of professional services and a Security Operations Center that's part of the Critical Insight Managed Detection and Response solution. Critical Insight helps organizations improve their entire security programs, not just one part.

Drex DeFord

Found of Rexico, LLC & 3xDrex.com
Former CIO Steward Healthcare, Seattle Children's, Scripps Health, USAF Health

Drex has over three decades of working in various senior leadership roles within the health information technology sector. He has delivered his expertise as a senior healthcare executive, a business/clinical strategist, a start-up CEO, and CIO, as a board director, and is a recognized digital health leader. Drex has broad and deep experience and expertise in healthcare providers' cyber security issues today and what they will face in the future. He is one of the Critical Insight Security Program creators for Critical Insight, where he holds the title of Healthcare Executive Strategist. You can connect with Drex on LinkedIn.

John Riggi

Senior Advisor Cybersecurity and Risk
The American Hospital Association

John is a highly decorated veteran of the FBI who spent almost three decades working to protect America from multiple threats and adversaries. He led the FBI Cyber Division national program to develop mission-critical partnerships with healthcare and other critical infrastructure sectors to ensure that these vital assets had protection from attack. John currently serves as the first senior advisor for cyber security and risk for the American Hospital Association and their 5000+ member hospitals. You can connect with John on LinkedIn.

JOHN RIGGI

The Cybersecurity Threat to Healthcare

I am fortunate to have served nearly three decades in the FBI. During that time, I had the opportunity to work on a variety of investigations ranging from international organized crime, money laundering, counterterrorism, counterintelligence, and finishing my career in the cyber division. Little did I know during my career that all those investigations and exposure to international criminals was delivering invaluable experience in understanding the nature of cyber threats and mitigating risks.

I realized cyber was not just a technological threat but is also another method of operation or "attack vector" for the same groups of international gangsters, terrorists, and spies I had been investigating for years. Cyber only enhanced the capabilities of these bad actors to successfully target US organizations, including healthcare providers.

Our focus in the FBI Cyber Division was preventing and investigating attacks on the US critical infrastructure, with particular attention on the healthcare sector. The FBI and DHS understand that the number one priority of cyber defense and investigation is preventing physical harm to people. We understand that ransomware attacks on hospitals are threat-to-life crimes because they directly threaten a hospital's ability to provide patient care and threaten patient safety. Unfortunately, this viewpoint was borne from necessity as hospitals and health systems have become a favorite target of ransomware attackers over the past several years. Hospitals can also suffer collateral damage due to attacks that spread uncontrolled over the Internet. The NotPetya attack in 2017, which started as an attack on Ukrainian infrastructure, spread globally and disrupted many hospitals and healthcare service providers coast to coast within the United States.

Healthcare remains one of the most highly targeted sectors by cybercriminals and nation-state actors due to its variety, volume, and accuracy of the multiple data sets. Healthcare is the only sector that combines PII, PHI, Payment Information, intellectual property, and national defense information. Each one of these data sets is uniquely valuable to cyber adversaries. In combination, they become exponentially valuable to cybercriminals for use in lucrative schemes, and to spies for intelligence objectives.

COVID-19 required the rapid expansion of remote technologies, a virtual work environment, and the connection of thousands of additional IoT and medical devices, expanding the attack surface for cyber adversaries. With the onset of the crisis, there was a dramatic increase in malware-laden phishing email campaigns directed toward the health care sector under the guise of important information related to COVID-19 or fake promises of N95 masks and other PPE for sale. Business email compromises (BEC) attacks, a common email related scheme to infiltrate security protections, have amplified in 2020. Cyber risk has dramatically increased with the exponential growth in remote work environments and the expanded use of telehealth due to social distancing requirements.

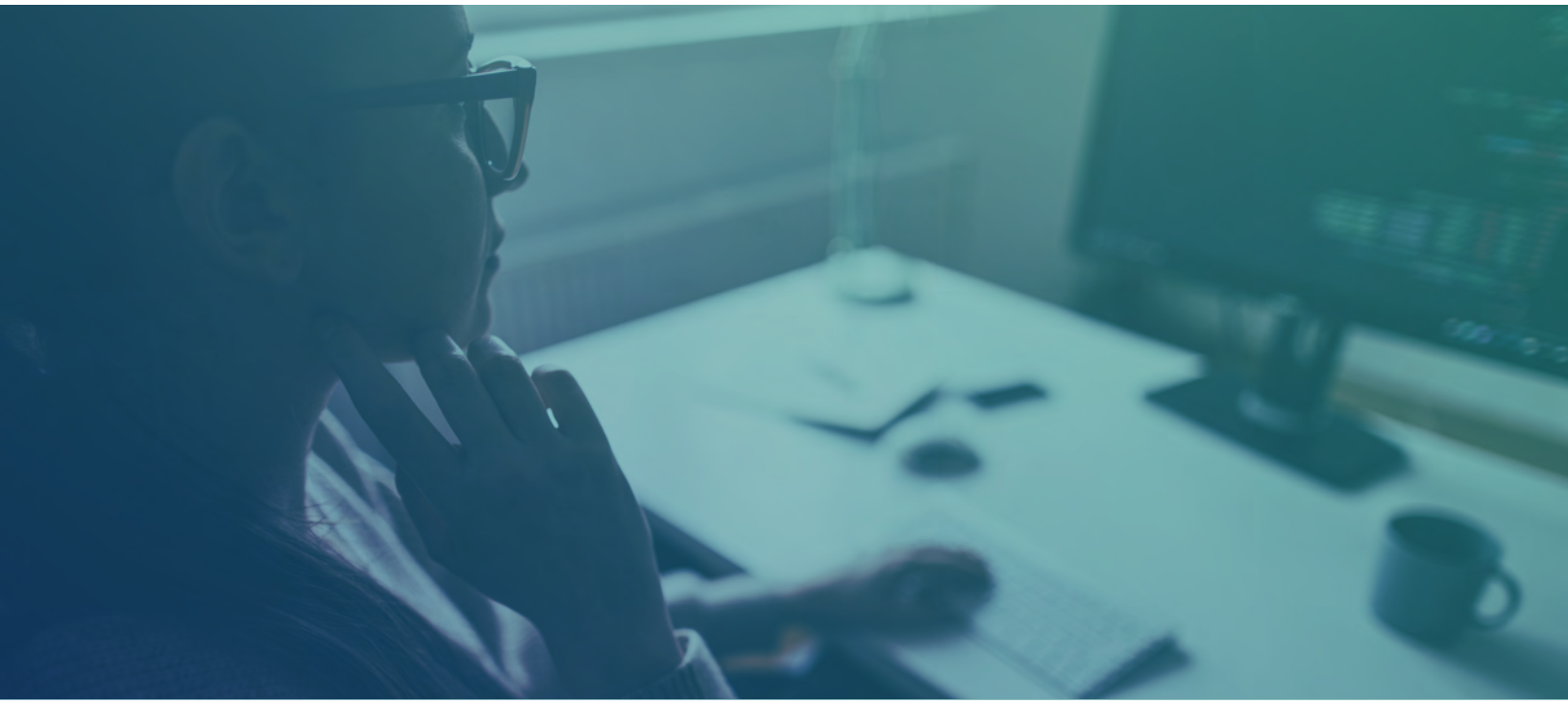
As healthcare cyber security teams face an onslaught of new threats, with tremendously increased demands on their expanded remote networks, they often become consumed and distracted by the daily tactical demands of protecting their networks and endpoints – the never-ending tackling and blocking. These necessary business-as-usual actions may distract the cyber security professionals and the organizational leadership from viewing cyber security from the strategic risk perspective and prevent them from guiding their organization along a successful security pathway that deals with current and emerging threats.

In this paper, Drex and I outline five cyber security areas that all healthcare providers and suppliers need to be aware of and address today.

DREX DEFORD

1. The Healthcare Cybersecurity "People" Problem

In smaller hospitals and clinics, we often task IT operations and development professionals with the additional duties of cyber security. This is a false economy as it distracts them from their core functions, and it puts non-experts in charge of protecting systems. Larger hospitals may have the resources to build an in-house security team staffed with cyber security experts. This is to be welcomed. However, with tight budgets and minimal margins impacting healthcare organizations of all sizes, it's tough to add new dedicated personnel to do these jobs, even if you can recruit them. At the end of 2019, it was estimated globally that the IT cyber security sector was four-million people short, with half of all current cyber-professionals saying their organization is at moderate or extreme risk due to staffing shortages.



Many healthcare providers also distract their limited IT security team further with dozens of additional projects each year and with ever-changing priorities. For example - new software implementations, upgrades to infrastructure, expanding facilities & buildings, dealing with acquisitions from an IT perspective, divestitures, integrating new medical equipment, or researching and discussing that cool new tool that one of the surgeons wants to try!

Everything works for a while. The distracted and taxed team runs all their regular operations, deploying and managing new projects, and taking care of all the organization's cyber security responsibilities. Until an unexpected pressure-test shows up. In the form of a surprise regulator or certification team visit, or maybe it comes in the form of a phone call from the FBI telling you they've found your organization's patient data on the dark web. Or, more recently, it comes in the form of the COVID-19 pandemic that changes the way the organization functions.

The staff pressure points become successful phishing attacks, ransomware infiltrations, or a stolen unencrypted laptop. Or it is attackers getting into an application or network because a patch wasn't applied to a switch or firewall. Even departed employees who weren't deleted from the network, so they're still accessing the organization's EHR. Or it could be a vendor-partner who was compromised by a hacker or malware, who then used their connection to get into your network and passed the infection to your systems. Or the piece of new medical equipment that was urgently added to the network for a clinical need that also brought along an exploitable cyber security vulnerability.

Nobody's perfect, and most IT professionals strive to deliver the best systems and security to their organizations. But a small, distracted staff, with cyber security added as an additional duty, can be especially vulnerable to mistakes and security issues in areas where they are not experts.

DREX DEFORD

2. The “Too Many Tools” Problem

We see the “too many tools” problem in every facet of our business, clinical, and research operations. Organizations buy great software or hardware tools because we’re told they will solve all our problems. Then we use only a fraction of the capability available in the new tools. This applies to everything we buy – from spreadsheet software, project management tools, to electronic health records, and more. We seldom use all the capability or functionality in any tool we implement.

In cyber security, we see the same problem, but with an even more complex personnel twist.

First, we buy many different cybersecurity tools, and we have a tough time linking the outputs and alerts together. So, logically, we buy tools to gather logs and alerts in one place. Realizing we don’t have the people, expertise, or time to review and fully act on the results, we do our best with the whole suite of complicated products and hope we don’t miss anything important.

Second, the situation is compounded by the lack of cybersecurity professionals. We buy the latest cyber security tool, then spend money and time to train a team member on how to use the tool. Armed with those new skills, our cyber professional has the opportunity to take a different job providing a higher salary. Our new tool delivered for a short while, but now we're headed to human resources to file a new job requisition. We might also have to spend money hiring a recruiter and more time and money training a new person on our staff to take ownership of the tool. In the meantime, our cool cyber security tool just sits there until we've filled the open position.

Third (and we've seen this way too often), a leader in the department leaves for a new job, and the replacement doesn't like the security tools the organization has in place. The new leader has honed their cyber security expertise using different tools than those you have at your organization. Following the "...and that's why they hired me – to make things better" maxim, those old tools become "shelf-ware", and new tools are purchased, staff are retrained, and the whole cycle starts over again.

"We buy the latest cyber security tool, ...staff are retrained, and the whole cycle starts over again."

Ultimately, this complex tool problem results in undocumented and unrecognized risk for the organization. While we may "have all the tools" and feel reassured by that, we should not be overly confident in our ability to get the job done. We may be lured into a false sense of security because we have all those great inventory tools, but they are not generating any actionable insights into the security picture, and the threats faced.

JOHN RIGGI

3. The Everything-is-Connected-to-Everything-Else Problem

Before COVID-19, healthcare was experiencing a connectivity and Internet of Things (IoT) revolution. Advancements and expansion in wireless technology, an increase in demand from consumers, and a culture of “smart” everything has translated readily into the healthcare sector. The growth of virtual networks, massive data centers supporting cloud services, wireless technologies with increased performance, speed, and cost reduction have driven business and consumer demands in all sectors, including healthcare. The COVID-19 patient surges and social distancing requirements were incredibly efficient at driving the need for remote technologies in healthcare, while also expanding the access points that cybercriminals can exploit.

Business, administration, and those involved in the spectrum of care are all network-connected these days to efficiently transfer patient data. Sometimes government regulations or payment models are implemented to achieve clinically integrated care, such as value-based payments and bundled payments, which are the drivers for vast transfers of patient data between organizations. All these connection points and data transfers are great for patients and clinicians to help improve outcomes, but they also increase vulnerabilities. Modern healthcare provision requires multiple connections between hospitals, vendors who supply and support clinical equipment, and remote telehealth provision to access experts and consultants in larger health providers. All increasingly delivered via software-as-a-service via public and private Cloud providers. All this expands the attack surface that cybercriminals can exploit.

“a culture of “smart” everything...expands the attack surface that cyber-criminals can exploit”

Facilities and security systems also take advantage of connected devices. It is common to enter a hospital and see wireless and network-connected security cameras, door access panels, TVs, printers, electronic message signs, point of sale terminals, refrigerators, vending machines, smart boards, and even fish tanks and coffee pots! Many modern facilities use network and internet connections to remotely monitor and adjust HVAC systems, water flow, power supply, lighting, and even sewage flow. There have been hospital breaches where hackers have penetrated main hospital networks through these “non information system” operation technology (OT) access points, such as an insecure gift shop POS terminal, which was not network segmented or misconfigured.

With the onset of the global pandemic, other drivers have greatly accelerated and magnified the demand for remote connectivity and increased the security risk.

These include:

- The cancellation of “elective” surgeries and medical appointments resulting in substantial revenue losses for providers.
- The massive, almost overnight, expansion of virtual private networks to accommodate a dispersed non-clinical workforce and third-party providers.
- Tremendous demand for telehealth visits and telemetry to provide remote health visits, preserve PPE for in-person visits, and allow clinicians to monitor patients remotely.
- An explosion of connected mobile devices by clinicians to record patient information and document care.

All these types of connections will continue to grow in the coming years as the COVID-19 accelerated demand for remote care and monitoring takes hold, and as 5G wireless technologies allow for many more wireless devices to be network connected with acceptable bandwidth and response times. Having a process to maintain an accurate, dynamic inventory, and patch status of all these network-connected devices will be a tremendous challenge in the near future. There will no longer be a traditional “network perimeter” to contain and manage network-connected devices. There will be a diverse, broad, and ever-changing connected mesh of medical and other devices that needs to be protected.

JOHN RIGGI

4. The “Culture of Cybersecurity” Problem

In the world of cybersecurity, practitioners often speak broadly about their risk reduction strategy in terms of “people, process, and technology”, with the emphasis often placed on process and technology vs. people. After all, wasn’t information security just an IT issue? Organizations believed that if they were compliant with HIPAA, they were secure from cyberattacks and regulatory exposure. Cybersecurity became an overhead function commonly limited to taking the mandatory annual 30 minutes “check the box” infosec course, even though malicious actors have found intricate ways to target the people and systems that are not discussed in most of these courses. This becomes a problem that requires new thinking and an aggressive willingness to embrace change that is a challenge for many organizations.

CIO/CISOs might see the urgency to change more clearly than many of their peers. And not to be too biased, but I think they might know how to adapt their organizations to the coming changes better than many other leaders. Mostly because they see and requirement. What also comes with being involved in organization-wide healthcare operations, unfortunately, is a front-row seat to the pervasive resistance to change.

For example, it is common for a hospital or health system to block 80 90% of all inbound email traffic as malicious or spam. Unfortunately, the many malicious emails that do get through the network defenses have fueled an explosion of successful cyber attacks over the past decade. There are millions of phishing emails enticing the recipients into “trusting and clicking” on an apparently benign email from Microsoft, UPS, Amazon, or other brands (September 2020 Microsoft’s Digital Defense Report). There is also a rise in credential phishing emails, where seemingly legitimate log-in pages appear requesting the end users’ name and password.

This demonstrates that it is the organization's people who can either be your best defense or weakest link against cyberattacks. One of the most effective ways to prevent and detect computer intrusions is through a top-down proactive cyber security culture, where every leader, staff member, and clinician feels it is their responsibility. If they are empowered to be part of the cyber security mission and staff. This requires a culture change.

One way to promote this top-down culture of cybersecurity in healthcare is to leverage the existing culture of care. Most people get involved in healthcare based upon some fundamental pre-disposition to care for those in need. Having staff and clinicians understand that the cyber security function’s priority is to preserve patient care and safety may go a long way in merging cyber hygiene with medical hygiene. The objectives of both are the same – the priority is minimizing risk to the patients and striving to ensure a positive outcome with the highest level of quality and safety.

In cybersecurity, protecting data security and privacy is very important and required under the law, but it is secondary to protecting the patients and the community. And instilling the culture of cyber security in everyone within the organization is key to protecting patients, their data, and the organization from regulators and lawmakers.

DREX DEFORD

5. The Cybersecurity in a Hurry Problem

The optimist in me wanted to believe the stories I read as far back as March that several hacker organizations had after the pandemic started, but pledged to lay off healthcare the pessimist in me was extremely doubtful. For good reason, as it turned out.

Conversations with CISOs at health systems across the country tell me they have been pounded by hacking, phishing, and ransomware attempts since the beginning of the pandemic. The bad guys have devised some remarkable scams associated with COVID-19, and cybersecurity leaders are working hard to hold the fort.

But we do worry about what's next given what has already happened. The COVID-19 emergency caused all healthcare providers to change business and clinical practices almost overnight. They rolled out work-from-home (WFH) for employees, drove exponential increases in telehealth visits, urgently acquired and installed (sometimes non-standard) equipment (including IoT/IoMT or other gear not following normal procurement processes). They extended capacity by quickly onboarding previously and retired clinicians and temporary employees. They added new locations for drive-thru testing, and connected to new suppliers to shore up the supply chain.

A lot was done in a hurry. This means we might have bypassed some of our best-practices for cyber hygiene in the name of mission support. And we did it with the best intentions – telling ourselves we'd go back and clean up the cyber issues later.

But what happens if later never comes?

Every discussion we've had with healthcare execs in the past three months suggests telehealth, WFH, and connections to new suppliers (including staffing, supply chain, and

business/clinical relationships) will continue into the future. Healthcare operations may very well have a “new normal”.

During this emergency, it is very likely that we laid a few landmines for ourselves. With long hacker dwell-time – the time the bad guys are in the network before they’re discovered - being measured in months, I wonder how many cybercriminals may have already breached networks or applications via well-written phishing emails, or via one of the new third-parties rushed through the security-vetting process. Are those hackers quietly exploring for our network’s data-crown-jewels, flying under the radar? It’s nice to imagine they’re “ethical” enough to hold off on springing ransomware in the heat of the pandemic. But even if they are, we know from experience, their ethics will eventually give way to greed.

And if many of the new clinical/ business practices we deployed during the crisis are the new normal for healthcare, we’ve definitely increased our cybersecurity risk level.

Summary

Healthcare providers have many factors that impact the delivery of health services to their patients. In addition to the surge in patient numbers and the changed working practices brought on by COVID-19, the population's underlying changing demographics and the rapid increase in new medical therapies place a strain on healthcare professionals and the insurance sector that funds the treatments. Add in the rapidly increasing threat landscape and other cyber security issues outlined in this paper, and it can be seen that hospitals and other healthcare providers have a lot to deal with.

Neglecting cybersecurity protections due to the overwhelming issues that are being faced is not an option. A single successful cyberattack could lead to very adverse patient outcomes if clinical systems are taken offline, or it could lead to ruinous financial and reputational complications if sensitive data is stolen.

Many organizations do not have the staff or the expertise in-house to protect against cyberattacks properly. As the healthcare system's load reduces due to the rollout of COVID-19 vaccination programs, a perfect opportunity will arise to review and

evaluate any cybersecurity protections in place. Both the recent rapid changes to IT provision made to deal with the new way of working, and the underlying protections that were already in place. It will be a perfect opportunity to audit current provisions, design a robust cyber security protection strategy, and implement various tools and tactics that can protect your organization today and into the future.

Engaging with external expert cyber security organizations will make sense for many providers in the healthcare sector. These external experts are entirely focused on existing and emerging cyber security threats, and they can ensure that your organization can avail of the latest intelligence, tools, thinking, and techniques. Adding outside expertise keeps your own internal IT staff from being distracted from their primary focus of delivering clinical and administration systems that keep the hospital or clinic functioning.

"Neglecting cybersecurity protections ... is not an option"

Many expert cyber security businesses are available to assist healthcare providers in securing and protecting their systems. The Critical Insight Security Program has the people, tools, and, importantly, the experience from real-world projects to help small to mid-size healthcare providers step-up their cybersecurity game. They provide assistance by elevating your entire security program, from 24×7 threat investigation to HIPAA Risk Assessments, Vulnerability Identification, Penetration Testing, and Anti-Ransomware programs. Their expert teams and consultants are ready, eager, and willing to assist your organization today.