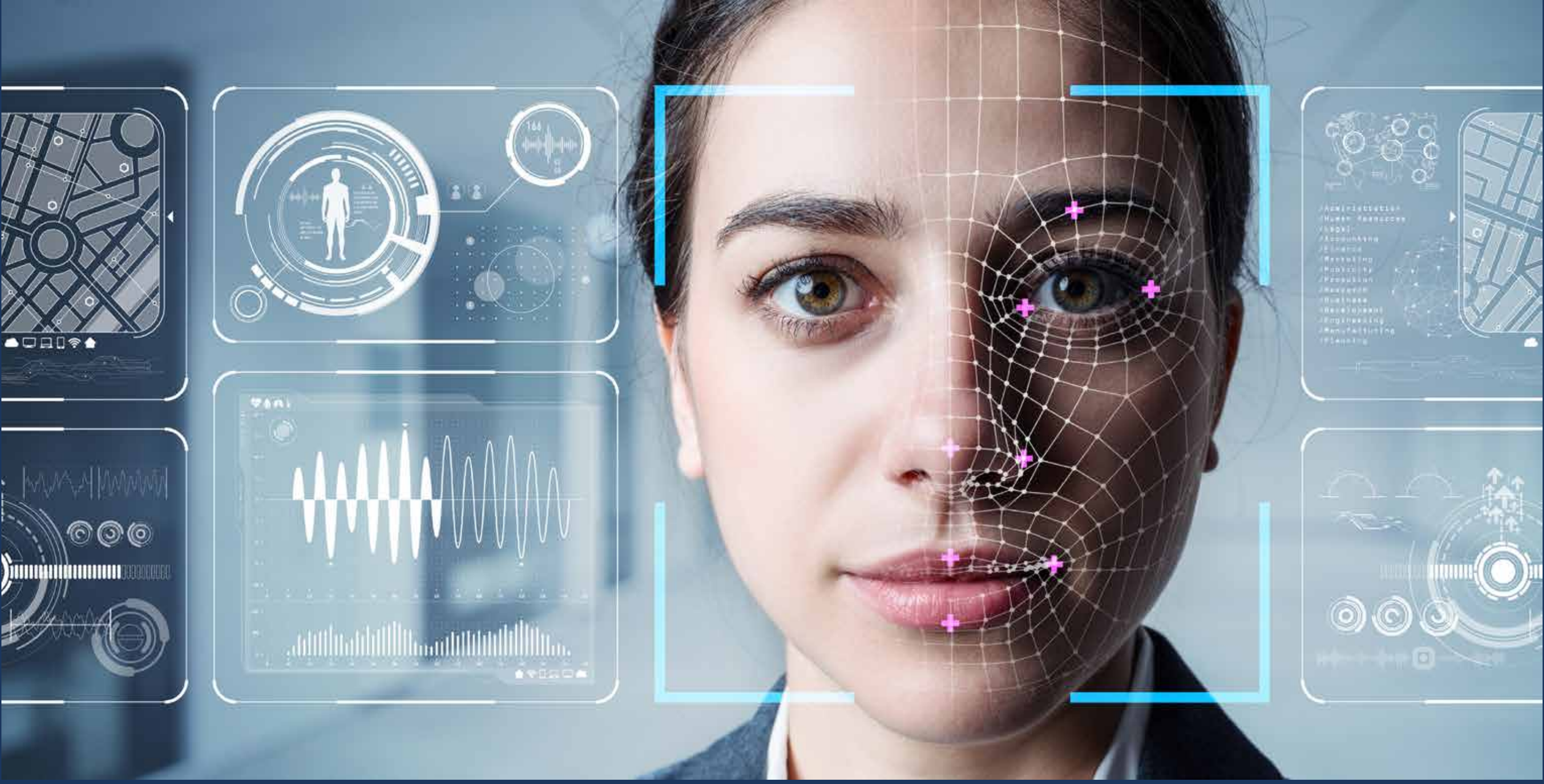
digital hands®

How to Prevent & Respond to Ransomware Attacks:

A Cybersecurity Playbook for Hospitals



INTRODUCTION

RANSOMWARE ATTACKS ARE THE 'NEW NORM'

The frequency of cyberattacks on healthcare institutions increases each year, but the COVID-19 pandemic and resulting expansion of telehealth services have made hospitals even more attractive prey for cybercriminals who know providers are not only willing to pay, but pay quickly, to recover from incidents that disrupt patient care.

Paired with the fact that an individual's medical records can be 20 to 50 times more valuable to hackers than personal financial information, it's no surprise that cybersecurity professionals in healthcare declared significant security incidents are now "the norm."

For healthcare providers, the consequences of a ransomware attack can be especially grave: the average incident costs $8.1 million, takes 287 days for full system recovery, and can jeopardize the quality of patient care for even longer than that.

The stakes are higher in healthcare because hospitals and large practices, as well as business associates that store and transmit data for hospitals, are subject to stringent HIPAA regulations. Various government agencies as well as the Payment Card Industry (PCI) also impose compliance requirements for data security standards, and the fallout—steep fines, litigation, a reputation dragged through the mud—can be so devastating it can result in permanent closure.

Unfortunately, cybersecurity leaders in healthcare are at a disadvantage due to a lack of proper security training for personnel, additional risk vectors from an increasing number of vendors and business associates, rising endpoints in the form of patients connecting to a multitude of networks, portals, and mobile devices, and finally, the fact that healthcare organizations themselves are not prioritizing IT budgets for security (one report found 82 percent of respondents dedicated 7% or less to the cause).

As demands become increasingly extortionate, with ransoms amounting to hundreds of thousands of dollars, it's critical to understand how to prevent, detect, and respond to ransomware incidents with the least amount of risk to operability.

In this playbook, we'll cover the actions you can take to improve the cybersecurity posture at your healthcare organization, including:

Five strategies you should set in place today to prevent a cyberattack tomorrow

The top tools and technology to prevent your organization from becoming another ransomware news headline

A breakdown of what to do in the aftermath of a ransomware incident

SECTION 1

THE TRUE COST OF A RANSOMWARE ATTACK

A healthcare provider's primary concern is to provide care, but having a vulnerable technology environment threatens operability, patient care, and revenue opportunities. Ransomware attacks happen when cybercriminals seize or encrypt data and refuse to release it unless an organization agrees to pay a sum of money for it, and repercussions can cripple patient care operations, whether an organization agrees to pay or not.

Remediations can easily cost hundreds of thousands of dollars—and an enormous amount of IT resources—depending on the severity and extent of the attack, and often far exceed the cost of the actual ransom. For example, since the University of Vermont Medical Center was attacked last October, it's racked up $1.5 million a day in lost revenue and recovery costs. Patient care ground to a halt and disruptions in departments ranging from radiology to sleep studies lasted for weeks.

Even worse, the one-time extortion attempt has evolved and become more sophisticated. Attackers regularly leverage ransomware to gain a persistent foothold in an organization's IT systems and control the data and return to ask for more ransom payments. Some may even refuse to release the data until yet more money is paid.

Ransomware by the Numbers

At least 560 U.S. facilities were impacted by ransomware attacks last year, with a spike of more than 45% in the final months of 2020.

- **24% of all ransomware attacks in 2020 were healthcare-related**
- **While the average ransomware payment is $233,817, many high-profile payments cost companies millions**
- **Email phishing represented more than 50% of ransomware attack vectors in the final quarter 2020**

The Biggest Loss to Businesses

- **21 days is the average downtime following a ransomware attack**
- **Downtime after an attack can cost 50x more than the ransom itself**
- **70% of ransomware attacks threaten to leak exfiltrated data**

SECTION 2

5 FUNDAMENTAL STRATEGIES TO IMPROVE YOUR CYBERSECURITY POSTURE

Many hospitals and medical facilities are woefully ill-prepared and ill-equipped to defend against the onslaught of ransomware.

87% of organizations don’t have proper personnel in place to defend against ransomware attacks

32% of hospital staff have never received proper cybersecurity training

7% or less of a healthcare provider’s IT budget is typically allocated for cybersecurity, compared to 15% or more in other sectors

To defend against the threat of ransomware, healthcare cybersecurity leaders must shift to a more proactive approach. **These are five fundamental strategies you should have in place today to prevent a cyberattack tomorrow.**

01 | Make sure the right people are leading cybersecurity efforts.

Most healthcare organizations have dedicated cybersecurity resources, but make sure there is also an organizational leader for this—someone with the 3 As: accountability if there is an attack; the authority to make changes; and enough time to pay attention to the issue.

That way, there are leaders within your organization who are prioritizing how to mitigate hypothetical cybersecurity incidents before they occur, working out response plans, and thinking through all of the worst-case scenarios so if the day comes, you and your people are ready.

***Pro tip:** If there is no CIO/CISO/CTO or Risk Officer, default to executive oversight by CFO with support of the strongest level of technical expertise on the IT team.*

02 | Develop a good response plan.

Have a formal incident response plan in place where every employee knows what to do and what the next steps are. The plan should include a playbook for containing ransomware damage, restoring services and data, as well as recovering from the attack.

A comprehensive plan should include law enforcement and regulator notification. It should also include a plan for managing publicity (PR) and victim notification. Don't forget to include the contact details of stakeholders like investors, practice owners, legal counsel, and third-party specialists who can come in and remediate.

***Pro tip:** If you're starting from scratch, a good reference is the Computer Security Incident Handling Guide from NIST, the National Institute of Standards & Technology.*

03 | Train your employees to avoid obvious traps.

Employee cyber-awareness training is an essential component of all cybersecurity defenses. Even if you are using cloud-based healthcare software to manage customer records, and the cloud provider's security team will actively work to protect patient records from attackers, it is still your responsibility to ensure that staff is trained to protect patient data.

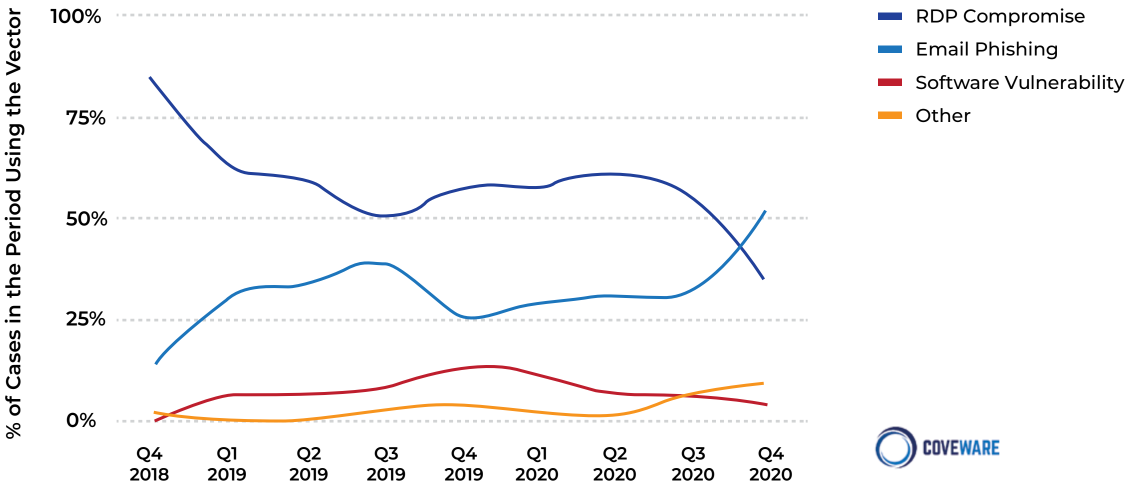
Ransomware most commonly finds its way into an organization attached to phishing emails that contain some sort of malicious attachment or link. If a staff member opens this attachment, the ransomware infects the PC, encrypting the data on it and spreading itself throughout the local network to do the same to other machines.

A very common attack vector for ransomware is compromised Remote Desktop Protocols (RDP). Many organizations fail to secure RDP services, which criminals use as a backdoor to exploit and access networks. Beyond minimizing RDP use as much as possible, make sure employees are creating passwords that are tough to crack.

Train your employees to be careful of which websites they browse, and how to spot emails that could be phishing. Hackers are increasingly improving the appearance of emails by masquerading as legitimate sources and brands, so improving security education and training around common and current threats should be a key focus.

***Pro tip:** For educational materials specifically designed to give HIPAA-covered entities and business associates insight into how to respond to a cyber-related security incident, check out references from the U.S. Department of Health & Human Services.*

● RANSOMWARE ATTACK VECTORS



04 | Regularly back up data and control who has access to it.

Although there are ways to prevent ransomware from infecting workstations, the easiest way to avoid paying a ransom to get data back is to back up regularly and securely so you can easily restore it.

Many ransomware attacks are crippling because a hospital has completely neglected to back up its data, making it extremely difficult to recover the data without paying the ransom. When you perform daily backups, you effectively insulate yourself from ransomware, which makes attacks a nuisance rather than a disaster.

Moreover, HIPAA requires that you carefully control access to patient data and ensure that only authorized employees can access it. This means staying on top of system audits and proactively removing access from terminated employees—and restricting RDP access to only employees who genuinely require it.

Pro tip: *To further minimize the risk of RDP compromise, use two-factor authentication and lock access after a certain number of failed log-in attempts.*

05 | Employ the right cybersecurity software and services.

In addition to a next-generation firewall, make sure you have up-to-date security software installed on all machines, including anti-malware detection with advanced endpoint protection. This is important because hackers can detect any out-of-date software or hardware that is connected to the internet using automated scanners, and then can use those vulnerabilities to infiltrate computers.

Indeed, almost half of data breaches at hospitals are reported to be ransomware attacks—and new research suggests many of those attacks could have been prevented with timely patching.

To get the security intelligence needed to detect and respond to incidents before they do major damage, you need the right solutions to effectively and rapidly action threat responses across your security infrastructure. In the next section, we'll discuss the most effective tools and technology you can adopt to mitigate the risks and consequences of a ransomware attack.

SECTION 3

SIX TOOLS THAT HELP DETECT AND PREVENT RANSOMWARE ATTACKS

As the pandemic continues, hackers will continue to target healthcare organizations. Healthcare leaders must shift to a more proactive security approach in 2021 if they hope to defend against ransomware attacks—and investing in the right cybersecurity technology should be a key part of any prevention strategy.

Having robust and integrated threat intelligence solutions will enable cybersecurity teams to react and respond faster to alerts and minimize damage from ransomware outbreaks. In addition to effective cloud security and vulnerability management software, here are six additional tools to help you:

Protect computing resources and remove infected workstations and medical devices from the network before the malware or ransomware spreads

Prevent third-party vendors from introducing vulnerabilities that must be successfully protected and monitored

Monitor your environment with highly effective Next Generation Security Incident and Event Management tools which can provide detailed alerts and analytics for anomalous and suspicious user and network activity

1

Next-gen SIEM

While rule-based legacy SIEM solutions generate many false positive alerts, next-generation SIEM platforms collect massive volumes of data in real-time and use patented machine learning algorithms to detect advanced attacks and flag anomalies such as insider threats and other hard-to-detect use cases. They can also provide AI-based security incident response capabilities for fast remediation.

2

Advanced end-point protection

Advanced endpoint protection solutions can "learn" to identify malicious files and activity based on the attributes of known malware. By continually monitoring all user and endpoint activity, it protects against malicious behavior by matching a stream of activity records against a set of dynamically updated attack activity patterns. Then, when a threat is identified, it can be immediately isolated at the endpoint to stop a ransomware outbreak.

3

Network traffic analysis

Cybersecurity leaders often struggle to detect sophisticated low and slow attacks which require monitoring a blend of network traffic activity, user actions, and system behavior patterns. With a platform that can monitor and correlate network traffic, security events, and user activities to detect the most advanced threats, you can quickly pinpoint and resolve security issues.

4

Web shielding

Security vulnerabilities in web applications are a significant risk that can be exploited, and outdated apps need to be protected from attacks and data breaches. Unfortunately, some can't be easily patched, and fixing vulnerabilities is a time-consuming and expensive process that often gets delayed, deprioritized, or even ignored. With web shielding services, you can monitor your web apps to provide protection, help you meet compliance challenges, and keep you secure during times of digital transformation.

5

Email cloud security

Conventional solutions built for on-premises email fail to adequately adapt for the cloud, and proxies and gateways are blind to compromised accounts and don't extend protection across connected applications like SharePoint. However, powerful cloud-based email security solutions can stop threats before they hit the inbox by monitoring threats and identifying hacker chatter. These tools offer the best defense against insider threats, business email compromise, and breached accounts since they can catch threats in connected cloud applications like OneDrive, Google Drive, and Teams.

6

Dark Web Monitoring

The dark web, deep web, and open web monitoring can identify threats to your organization or data that has been breached. Getting a monitoring service that aligns your intelligence program to your unique risk profile and delivers actionable and relevant intelligence with recommendations for risk mitigation will accelerate protection from ransomware and phishing attacks.

SECTION 4

THE TOP RANSOMWARE QUESTIONS, ANSWERED

No matter how prepared you are, a hacker may still find a hole in your security. In the unfortunate event an attack does happen, then what?

These are the top questions you'll need answers to in the aftermath of an incident.

01 | Who should I call first?

Your general counsel is your first call if you trust that he or she knows the legal ins and outs of cybersecurity law and is on the list of parties you will get reimbursed for through your ransomware insurance policy. Otherwise, call your cyber insurance broker. (And after that, go to law enforcement to file a report.)

02 | What is the most responsible disclosure strategy?

First off, call it an incident or event, not a "breach," which is a legal term that indicates a far more severe situation.

The fact is, you should have developed and adopted a responsible disclosure policy and made it publicly available, so ethical hackers and the information security community know that you are responsible when dealing with security disclosures.

Apart from laws and HIPAA regulations that mandate when you need to report incidents to others, you should check if you have obligations to vendors that contractually may require immediate disclosure. At times, that may be impossible, so you'll need to discuss with your counsel about those cases.

03 | If I decide to pay the ransom, is there a right way to do it?

Never make the ransom payment yourself. Ransomware negotiations are not the same as a lease or contract negotiation. Cybercriminals don't respond to the same rational arguments, and things can easily go off the rails.

If you decide to pay a ransom, work with a vendor who can make the payment in bitcoin in a legal way, and give you the information you need to be comfortable. The payer needs to be on an approved list from the U.S. Treasury Department and should agree to file a Suspicious Activity Report (SAR) to FinCEN, the Financial Crimes Enforcement Network bureau. Separately, you should also report to law enforcement when the payment happens.

04 | What fines do I need to worry about?

The Treasury Department's Office of Foreign Assets Control (OFAC) has a list of terrorists you can't pay—if you do, you'll be fined. FinCEN also has guidelines for how approved vendors need to register and report ransom payments.

Individual states may also fine an organization for not reporting an incident in a timely manner; for example, if a hospital knew about an incident but didn't report it at the time.

The key takeaway is that the more communication you have with law enforcement and regulators as a situation develops, the less likely you are to face fines later on.

05 | How can I ensure I'll be reimbursed by insurance?

Most insurance carriers won't give you a hard time; but when they do, it's often because of late reporting. When an incident goes unreported during the policy period during which it happens, but it incurs costs and consequences later, the insurer may not reimburse you for it.

Another common reason is picking a vendor that isn't on the carrier's approved list, so make sure you have approval beforehand. In rare cases, there may also be a rate issue if you hire someone at a higher-than-average cost, and the insurer will make you cover the difference.

06 | After I pay, does it mean I'm safe?

Even after paying the ransom, you need to continually guard your live environment. When 2.0-type ransomware gets in your network systems, it's as sophisticated as an e-discovery vendor, but looking for embarrassing C-suite emails, invoices, and credit card billing information. And if you haven't closed the window, hackers could definitely be back.

CONCLUSION

ENSURE YOUR DATA IS SECURE WITH DIGITAL HANDS COMPOSABLE SECURITY

According to Ponemon, one of the best ways to minimize the impacts of ransomware is to use a managed security service provider (MSSP) to help close the security skills gap.

It doesn't take long to properly secure your healthcare organization, but it does require well-thought-out policies and a plan. It also requires that you have dedicated IT resources. Keeping crucial data like patient records and billing information secure is no easy feat for even the largest healthcare providers. HIPAA regulations require network, IT infrastructure, and cloud services monitoring 24x7x365 across all endpoints, firewalls, and access points—which is beyond the capability of many IT teams.

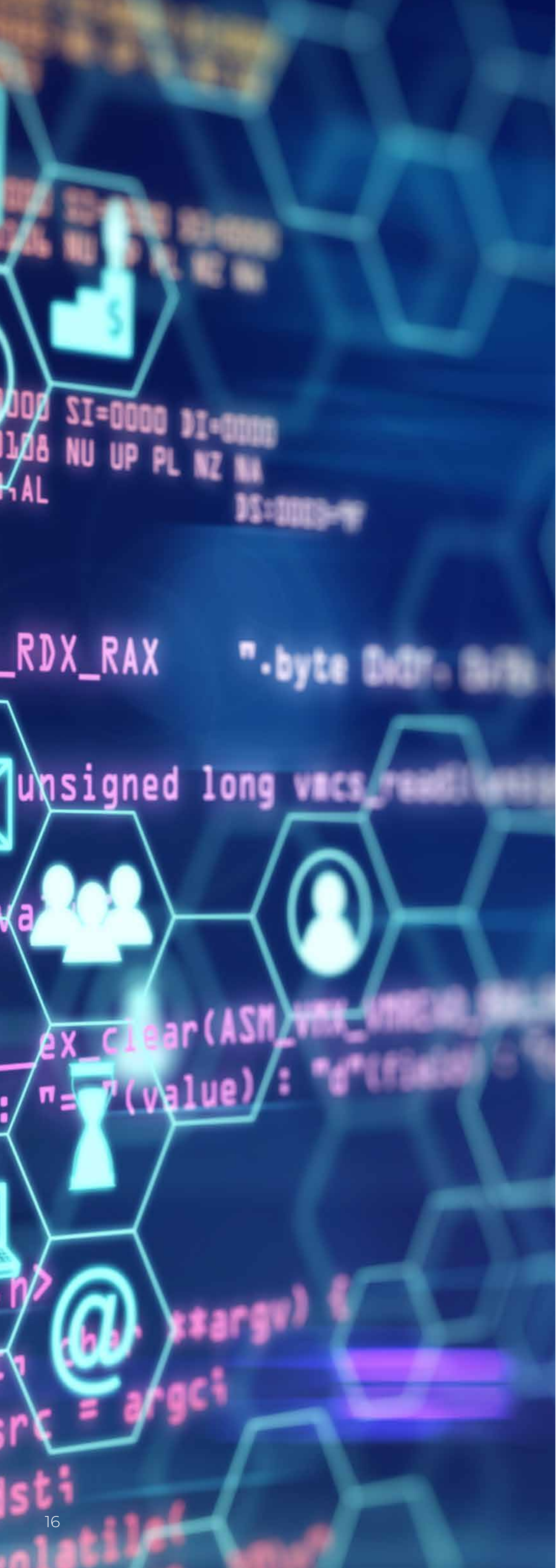
When healthcare providers can't find (or retain) the right resources, the risks of a successful cybersecurity attack are heightened. Someone who isn't a cybersecurity professional may have read all the articles and followed all the guidelines, but will still miss things.

When healthcare providers can't find (or retain) the right resources, the risks of a successful cybersecurity attack are heightened.

In fact, even if you have multiple internal resources, it's still advisable to place a specialized cybersecurity responder on retainer. It's not a one-size-fits-all environment anymore, and a good specialist will be able to help put a response team together, initiate immediate remediation in the event of an attack, get systems back online, support negotiations, restore systems, and prevent future incidents.

Partnering with a good MSSP can also ensure compliance with cybersecurity-first processes and practices, and even support the training of staff on the secure handling of patient data. As a tech-agnostic MSSP, Digital Hands improves cybersecurity in the healthcare industry with a unique "composable security" platform that can be customized to your organization's specific needs.

Get in touch at
(855) 511-5114 or sales@digitalhands.com.



ABOUT DIGITAL HANDS

Digital Hands is a trusted, award-winning cybersecurity leader with extensive security expertise offering advanced protection, detection, and remediation services. Digital Hands' Composable Security Model optimizes legacy security infrastructure while augmenting with today's latest security solutions to safeguard your organization against ever-present cybersecurity threats around the clock, anywhere in the world. To learn more, please visit www.digitalhands.com.

digital hands®

www.digitalhands.com
(855) 511-5114
4211 West Boy Scout Boulevard Suite, 700 Tampa, Florida 33607
sales@digitalhands.com