CYVATAR.AI

2021

STATE OF EMERGENCY:

CYBERSECURITY IN HEALTHCARE

BY: CRAIG GOODWIN + COREY WHITE

cyvatar.ai

STATE OF EMERGENCY:

CYBERSECURITY IN HEALTHCARE

TABLE OF CONTENTS

INTRODUCING THE

UNF**KING CYBERSECURITY COMIC SERIES

By Cyvatar

This is not your average eBook! We created a nine-part comic series for each chapter's theme. Sit back, relax, and enjoy a bit of comic relief. And if you get a laugh, feel free to take a screenshot and share it on social media—tag us @cyvatar!

DRAMATIS PERSONAE:

Comic strip illustrated by **Matt Bradshaw for Cyvatar**


CISO


DENTAL HYGIENIST


DENTAL PATIENT


DENTIST


HACKER


HCO REP


HOSPITAL ADMIN 1


HOSPITAL ADMIN 2


HOSPITAL CEO


LOCAL DOCTOR


MEDICAL STAFF 1


MEDICAL STAFF 2


MEDICAL STAFF 3


MEDICAL STAFF 4


MSP REP


NEW HOSPITAL CEO


OFFICE MANAGER


OUTSOURCED IT


PATIENT 1


PATIENT 2


PATIENT 3


PATIENT 4

GLOSSARY OF ACRONYMS

APT	Advanced persistent threat
BEC	Business email compromise
CIS	The Center for Internet Security
CISA	The Cybersecurity and Infrastructure Security Agency
CSA	The Cloud Security Alliance
EHR	Electronic health records
EMR	Electronic medical records
HCIC	The Healthcare Internet Conference
HCO	Healthcare organization
HHS	U.S. Department of Health and Human Services
HICP	Health Industry Cybersecurity Practices
HIMSS	Healthcare Information and Management Systems Society
HIPAA	The Health Insurance Portability and Accountability Act of 1996
HITECH	The Health Information Technology for Economic and Clinical Health Act
HITRUST	The Health Information Trust Alliance
HR	Human resources
ITR	The Verizon Insider Threat Report
MHR	Medical health records
NIST CSF	The National Institute of Standards and Technology Cybersecurity Framework
OCR	Office of Civil Rights
PHI	Protected health information
PII	Personally identifiable information
SLTT	State, local, tribal, and territorial governments

TL/DR:

THIS BOOK IN A NUTSHELL

2020 was a year for healthcare breaches like no other. Phishing attacks, ransomware, and business email compromise (BEC) all had an outsize **effect on healthcare organizations** (HCOs), in part as a result of factors stemming from **the COVID-19 pandemic.**

2020 HEALTHCARE BREACHES

Hackers around the world had a field day playing off patient fears and system vulnerabilities alike—here's a look at some of the biggest[1]:

01 3,320,726 PATIENTS AFFECTED

TRINITY HEALTH: Trinity's breach stemmed from a cyber attack on its philanthropy database vendor, Blackbaud, in which millions of patient and donor records were exposed. In a security notice, Blackbaud said that it had paid the ransom to have the data copy destroyed—a strategy security experts do not advise.

02 1,045,270 PATIENTS AFFECTED

INOVA HEALTH: Inova was affected by the same Blackbaud security incident. The Virginia-based system determined that the threat actor may have accessed personal information of patients and donors.

03 1,013,956 PATIENTS AFFECTED

MAGELLAN HEALTH: The Arizona HCO discovered it was the victim of a ransomware attack; an investigation revealed that the incident may have affected personal information.

04 1,004,304 PATIENTS AFFECTED

DENTAL CARE ALLIANCE: The Florida-based support organization, which is affiliated with more than 320 practices in 20 states, reported this fall that it had been the victim of an ongoing attack.

05 829,454 PATIENTS AFFECTED

LUXOTTICA OF AMERICA: Luxottica of America, which operates vision care facilities, was targeted by class-action lawsuits following the breach of its online scheduling application.

[1] Data adapted from Jercich, Kat. "The biggest healthcare data breaches reported in 2020." Healthcare IT News. December 30, 2020.

HCOs often struggle with competing priorities that affect patient safety, profitability, standard and efficacy of care, and more. Our goal in writing this book is to show that you can meet your business and cybersecurity requirements without sacrificing one for the other.

But you'll have to change the way you look at and control for risk to succeed!

We know change is painful. We know it's hard to recognize when change is imperative—because we've been there. We've experienced all of the scenarios in this book, we've made mistakes, we've lost value, we've been duped by vendor false promises. We've been in the trenches and believe passionately in building better alternatives.

We believe that if you challenge yourself, your organization, and your partners to make the changes necessary to ensure you achieve successful business and patient outcomes, you'll regain your agency and boost your security confidence.

The book walks through a number of well-known cybersecurity challenges in the healthcare industry and offers guidance to help you achieve measurable time to value every step of the way. It wraps with a six-point checklist and a plan to help you move forward with a successful cyber strategy, regardless of where you are in your security journey.

We believe in the power of transformational change to create unprecedented outcomes. This book will help you achieve them.

– Corey + Craig

FOUNDERS

CHPTR
01

VULNERABILITY 911:

HEALTHCARE ORGANIZATIONS ARE MORE SUSCEPTIBLE TO CYBER ATTACKS THAN MOST

UNF**KING CYBERSECURITY by CYVATAR.AI

We like to kid, but this is no joke: From small independent practitioners to large hospital environments, attacks on healthcare records, IT systems, and medical devices have infected even the most hardened systems, exposing sensitive patient information and leading to substantial financial costs to regain control of systems and patient data.[2]

To illustrate this problem at a glance, we've adapted the FLACC scale to reflect levels of cyber pain across the industry:

FLACC SCALE

0: RELAXED AND COMFORTABLE:

While it may be true in some circumstances that ignorance is bliss, **when it comes to cybersecurity, what you don't know *can* hurt you.** There are more statistics out there regarding security risks in healthcare than we can cover in this book, which can lead to desensitization of the problem and make it easy to ignore cyber threats to "focus" on patient safety. However, as we will show, cybersecurity should actually be a priority for patient safety, and this is true regardless of the size of your organization or which part of the industry you belong to. Relaxed and comfortable will get you breached.

4 TO 6: MODERATE PAIN:

Complex and conflicting compliance requirements are painful indeed, and HCOs—like your counterparts in other industries—often make the mistake that full compliance means you have full security, but that couldn't be further from the truth. **A strong, resilient cyber strategy will deliver compliance as a natural byproduct, but it doesn't work the other way round.** We'll take a look at ways to navigate HIPAA, HITRUST, and HITECH to help you achieve better cyber protections and patient safety at the same time.

1 TO 3: MILD DISCOMFORT:

Disparate networks—patient, clinical, business—are a thorn in the side of healthcare organizations (HCOs); **the problems that arise from one network's inability to communicate safely and effectively with another is further compounded by too many IT and security providers in the mix** and ageing hardware and software that may be too old to qualify for vendor technical support. Wireless and IoT devices open the door to even more vulnerabilities, setting your organization up for more intense pain.

7 TO 10: SEVERE DISCOMFORT/PAIN:

Ransomware, anyone? Anyone? **Fallout from ransomware or any other type of cyber attack comes with a high price tag, whether you choose to pay the ransom or not.** Post-attack remediation is costly and time consuming and in many cases leads to system slowdowns or shutdowns that can adversely affect patient safety. With U.S. healthcare spend at more than $3 trillion annually—that's trillion, with a "t"[3]—the more than $125 billion expected to be spent on cybersecurity by 2025 is barely a third of what it should be to combat these threats effectively.[4]

[2] Decker, Eric C. and Julia Chua. "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients." HHS. Page 5.

[3] Morgan. Steve. "Healthcare Industry To Spend $125 Billion On Cybersecurity From 2020 To 2025." Cybercrime Magazine. September 8, 2020. That estimated $3.5 trillion in annual spend is 18 percent of the U.S. gross domestic product and the highest in the world among developed countries. Yikes!

[4] Especially when you consider HCOs suffer up to three times more cyber attacks than financial services companies—and those orgs spend an average of 10% of their IT budgets on security initiatives according to research by Deloitte. In other words, HCOs receive three times more attacks but spend three times less on protecting against them. Former prosecutor Lisa Rivera's estimates on industry spend are even higher; in a recent Cybersecurity Ventures report, she notes that four to seven percent of a health system's IT budget is spent on cyber, compared to about 15 percent for other sectors like financial services. Double yikes!

Add to which, the widespread adoption of a false if-it-ain't-broke-don't-fix-it mentality (think "relaxed and comfortable") and a general lack of understanding that security technology is—or in any case should be—an integral part of patient care contributes heavily to the large number of vulnerabilities, as does the outsize influence of many doctors on their HCO's technology-related decisions.

A doctor who is important to a hospital's ranking or reputation, for example, may dictate the retention of older, outdated systems because of an established comfort level with those solutions or a lack of understanding the benefits of changing to newer, more efficacious tools. And of course, HCOs are also more prone to attacks than other industries because they persist at managing through breaches reactively.[5]

The increased vulnerability of HCOs to cyber threats can be blamed on outdated IT systems, the lack of robust security controls, and insufficient IT staff, while valuable medical and health data—and the need to pay ransoms quickly to maintain access to that data—make healthcare targets popular and relatively easy to breach.

LESSON 01

And if all that's not sobering enough, consider:[6]

MORE THAN 93% of HCOs have experienced a data breach over the past three years

57% have had more than five data breaches during the same time frame

NEARLY 75% of HCOs reported that their infrastructures are unprepared to respond to attacks, representing a 300% increase in vulnerabilities over last year

96% believe attacks outpace their security investments

[5] Help Net Security. "Healthcare organizations are sitting ducks for attacks and breaches." HelpNetSecurity News. November 16, 2020.

[6] Data adapted from: Cobel, Sarah. "Healthcare Data Breaches to Triple in 2021." Infosecurity Magazine. November 16, 2020; and Op cit. "Healthcare organizations are sitting ducks;" and Op cit. "Healthcare Industry To Spend $125 Billion On Cybersecurity."

As a result, only 14 percent of hospitals and just six percent of physician organizations believe their cybersecurity will show improvement from 2020 levels; fully 26 percent of providers admit their cybersecurity has worsened.[7]

Which means the cybersecurity industry itself can actually contribute to the problem. For more than 30 years,[8] cyber attacks have grown across every sector, including healthcare, and the security industry has failed to keep pace with the adaptability of today's cyber criminal. Vendors use fear, uncertainty, and doubt (FUD) to fuel purchases of the latest security tools in an attempt to keep personal health information (PHI) safe. And almost nowhere is this approach as compelling as it is in healthcare, where more than credit card data is at risk.

Healthcare organizations face additional hurdles stemming from legacy systems that are no longer supported by the companies that built them, so there are no patch management options available to keep them secure.

HCOs haven't sufficiently updated their security strategies and the tools that manufacturers, IT software vendors, and the FDA have made haven't been robust enough to thwart the more sophisticated techniques of threat actors.

LESSON 02

"When I complete health questionnaires, what happens? What if they type something wrong in the computer? It would be nice to know how they keep my data confidential. It's scary enough just having to see a doctor—I don't want to have to worry about the documentation I leave with them too!"

PATIENT Pat

[7] Ibid.

[8] Since1989 and the first reported computer virus, created by Robert Morris.

Healthcare organizations face additional hurdles stemming from legacy systems that are no longer supported by the companies that built them, so there are no patch management options available to keep them secure. **Unlike other industries that can migrate data and sunset old systems, limited IT and security budgets at HCOs make migration difficult and potentially expensive, particularly when an older system provides just one small—but unique—function or houses data necessary for compliance or research, but didn't make the cut to transition to a newer system.**

Which explains why, even though the amount of dollars spent on healthcare cybersecurity is increasing, 82 percent of hospital CIOs and 90 percent of practice administrators surveyed by HelpNetSecurity admit they are not even close to spending an adequate amount on protecting patient records from a data breach.[9]

We know hackers are always evolving and becoming more sophisticated, making it imperative that HCOs find newer and more innovative ways to improve patient safety by reducing risk to healthcare systems.

Woefully inadequate security controls, weak or shared passwords, code-based threats, and other vulnerabilities expose HCOs to bad actors intent on illegally accessing treasure troves of patient data.

LESSON 03

The U.S. Health & Human Services Office of Civil Rights shines a bright light on the gap by publicly reporting any disclosed breaches that affect more than 500 patient records, and other government agencies lend a hand to help secure vital PHI. In the last quarter of 2020, three U.S. government agencies (CISA, the FBI, and HHS) issued a joint cybersecurity advisory alerting HCOs of an imminent cyber threat. They warned of malicious actors targeting the healthcare sector with Trickbot malware that could lead to ransomware attacks, data theft, or the disruption of healthcare services.[10] The advisory went on to encourage companies to review and update their business continuity plans so they could execute essential functions in the event of a cyber attack.

[9] Op cit. "Healthcare organizations are sitting ducks."

[10] National Law Review. "Multiple Federal Agencies Jointly Warn of Increased and Imminent Cybercrime Threat to U.S. Hospitals and Healthcare Providers." October 2020.

WHAT YOU CAN DO TODAY

01 Start by prioritizing your electronic health and medical records (EHR and EMR) to ensure your most sensitive and important records are safe.

02 Identify which, if any, of your operating room or emergency department systems fall outside core electronic health records. Hackers always look for weak links, and old legacy systems can serve as common gateways for them to infiltrate.

03 Catalog and prioritize all medical devices. Devices that, according to the FDA, "usually sustain or support life, are implanted, or present a potential unreasonable risk of illness or injury," are by definition high priority. Patient safety and clinical risk management teams can help prioritize the rest.

04 Scan and patch all operating systems, software, and firmware routinely.

05 Keep your software—especially antivirus and anti malware tools—updated.

06 Change network passwords regularly and implement multifactor authentication tools.

07 Audit user accounts regularly, especially those with administrative privileges, to remove unnecessary privileges and disable unused accounts.

08 Create offline backups of critical assets.

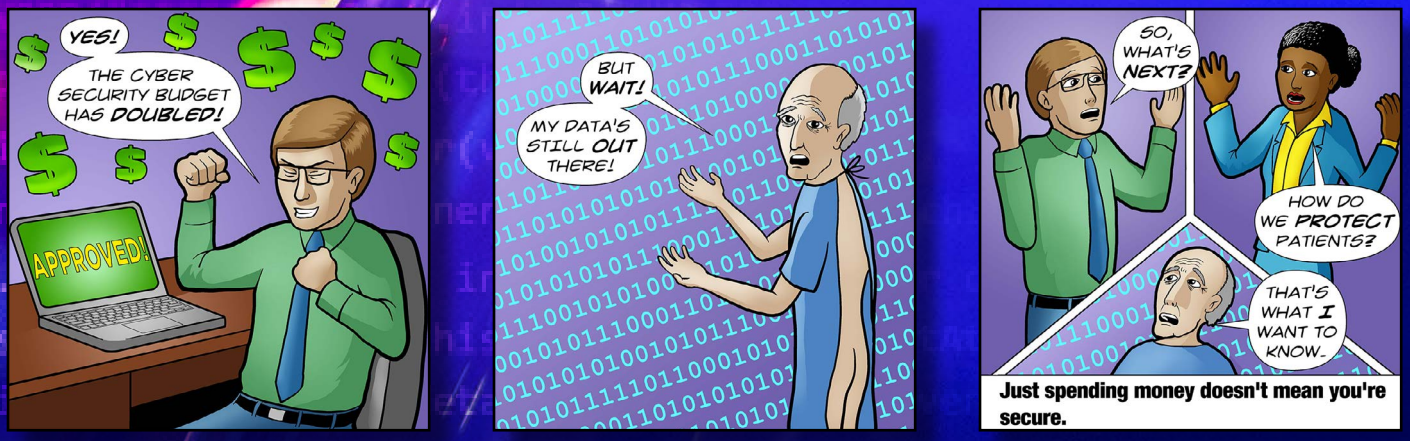
09 Segment your network to prevent hackers from hitting the mother lode through a single vulnerability.

Given the increasingly sophisticated and widespread nature of cyber attacks, the healthcare industry must make cybersecurity a priority and make the investments needed to protect its patients.

Like combatting a deadly virus, cybersecurity requires mobilization and coordination of resources across myriad stakeholders including hospitals, IT vendors, medical device manufacturers, and government entities to mitigate the risks and minimize the impacts of a cyber attack.[11]

[11] Op cit. "Health Industry Cybersecurity Practices."

CHPTR
02
LIES, DAMN LIES, AND STATISTICS



UNF**KING CYBERSECURITY by CYVATAR.AI

Putative facts and figures are hardly in short supply in any industry, and healthcare stats are no exception. With the healthcare industry estimated to spend just $134 billion on cybersecurity by 2026, 82 percent of CIOs and CISOs agree that the dollars thus far have not been allocated effectively, often spent only after breaches occurred and without a full gap assessment to help prevent future incursions.[12]

In healthcare, a cybersecurity incident isn't just about losing data or exposing PHI—it also has life-threatening impacts. System downtime resulting from cyber attacks affects an HCO's ability to treat and see patients, so patient lives are literally at stake.

IT research firm Gartner predicted that more than 25 percent of 2020 cyber attacks in healthcare would involve the Internet of Things (IoT).[13] In medical terms, that means wirelessly connected and digitally monitored implantable medical devices (IMDs)—such as cardioverter defibrillators (ICD), pacemakers, deep brain neurostimulators, insulin pumps, ear tubes, and more,[14] opening a whole slew of new attack vectors.

Additionally, Kim Zetter of the Washington Post wrote that researchers in Israel had created a computer virus capable of adding tumors to otherwise clean CT and MRI scans—malware designed to fool doctors into misdiagnosing high-profile patients—which is perhaps the shape of things to come for HCOs that continue to lag in their cyber strategies.

25% OF 2020 CYBER ATTACKS IN HEALTHCARE WOULD INVOLVE THE INTERNET OF THINGS (IoT).

- Cardioverter defibrillators (ICD)
- Digitally monitored implantable medical devices (IMDs)
- Deep brain neurostimulators
- Insulin pumps
- Pacemakers
- Ear tubes

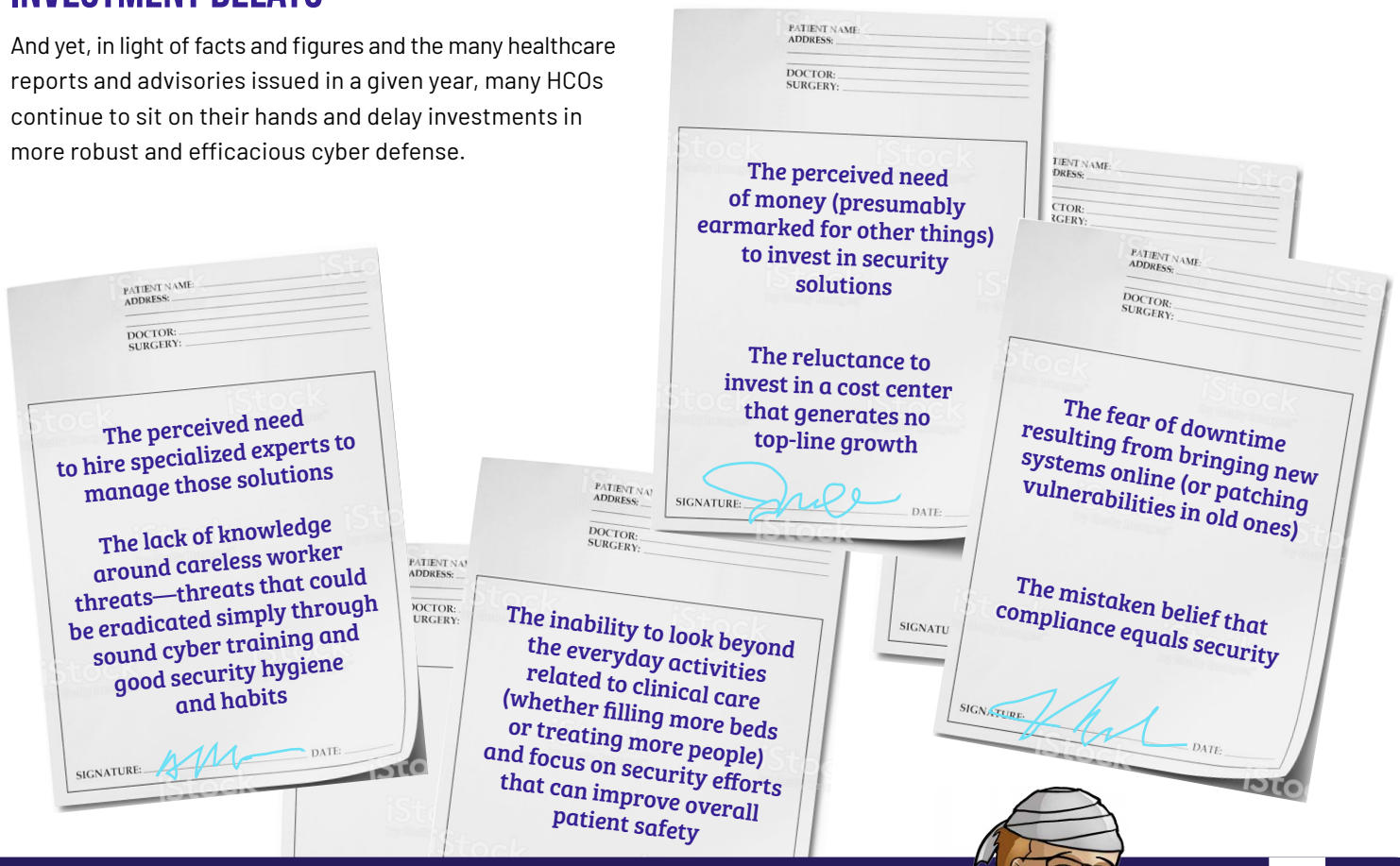
[12] Op cit. "Healthcare organizations are sitting ducks."

[13] Kathy Hughes, CISO at Northwell Health, one of the nation's largest healthcare systems, told Cybercrime Magazine that IoT devices are, in her opinion, computers with operating systems (OS), similar to other types of computers—and those devices are susceptible to the same cyber threats. She added that IoT devices have a small OS and that security is a bolt-on rather than built-in, which is problematic in and of itself.

[14] Op cit. "Healthcare Industry To Spend $125 Billion."

REASONS FOR CYBERSECURITY INVESTMENT DELAYS

And yet, in light of facts and figures and the many healthcare reports and advisories issued in a given year, many HCOs continue to sit on their hands and delay investments in more robust and efficacious cyber defense.



"My hospital had a ransomware attack! They are diverting patients to another hospital, but it's out-of-network and expensive. Is it safe for me to postpone my procedure? And if the hackers stole my medical records, will I still be able to receive treatment? Help!"

PATIENT Pat

Throw in lots of different security vendors and solutions, the ease with which an HCO can fall out of compliance with standards like HIPAA, and mounting risks from unremediated system vulnerabilities and you have a perfectly enticing attack environment on your hands.

But you don't have to take our word for it! Just the first quarter of 2021 offers plenty of evidence[15]:

500,000 MEDICAL RECORDS

In February, nearly 500,000 medical records of French residents appeared online, believed to have been stolen by hackers from multiple French HCOs. **Names, medications, fertility details, and blood type are among the exposed data elements.**

45,000 PATIENT DATA

Saginaw, Michigan-based Covenant HealthCare notified 45,000 patients that their **data, including clinical information and diagnoses,** is at risk after two employee email accounts were hacked in May 2020.

586,869 + 157,939 PATIENTS

Meanwhile, data breaches from the Accellion and Netgain hacks also continue to climb:

- Trinity Health: **586,869 individuals affected**
- Woodcreek Provider Service: **Undisclosed**
- CalViva Health: **Undisclosed**
- Allina Health Apple Valley Clinic: **157,939 patients that their medical, financial and contact data was compromised**

SPECIAL REPORT

[15] Ibid.

"I can't believe my data is so vulnerable! Who are these hackers and what are they doing with my health records? I always trusted my doctors to protect my privacy—how can I continue to trust them with my health if they can't even keep my records safe?"

PATIENT *Pat*

Data breaches related to COVID-19 scams are also through the roof, says The Wall Street Journal's Brooke Henderson. **U.S. officials have analyzed almost 80,000 COVID-19 domain names looking for fraud and made multiple arrests, including those of three men who allegedly tried to sell doses at an impost or Moderna website.**[16]

The FBI's 2020 Internet Crime Report corroborates all of this and more, with data that show cyber attacks the U.S. public reported to the agency last year surged in number and value.[17] There were $4.1 billion reported losses from cybersecurity incidents, up 20 percent from 2019 and 791,790 logged complaints—a 69 percent increase. Other data include:

LESSON **04**

Remember: HCOs experience very particular security challenges, not because the cyberattacks are unique, but because of what's at stake.Excuses will get you breached.

	# OF INCIDENTS
Phishing scams:	241,342
Identity theft:	43,330
Business email compromise:	19,369
Tech-support fraud:	15,421
Ransomware:	2,474

[16] Mathews, Anna Wilde. "Major Hospitals Form Company to Capitalize on Their Troves of Health Data." The Wall Street Journal. February 11, 2021.

[17] Rundle, James. "Hospitals Suffer New Wave of Hacking Attempts." *The Wall Street Journal.* February 2, 2021.

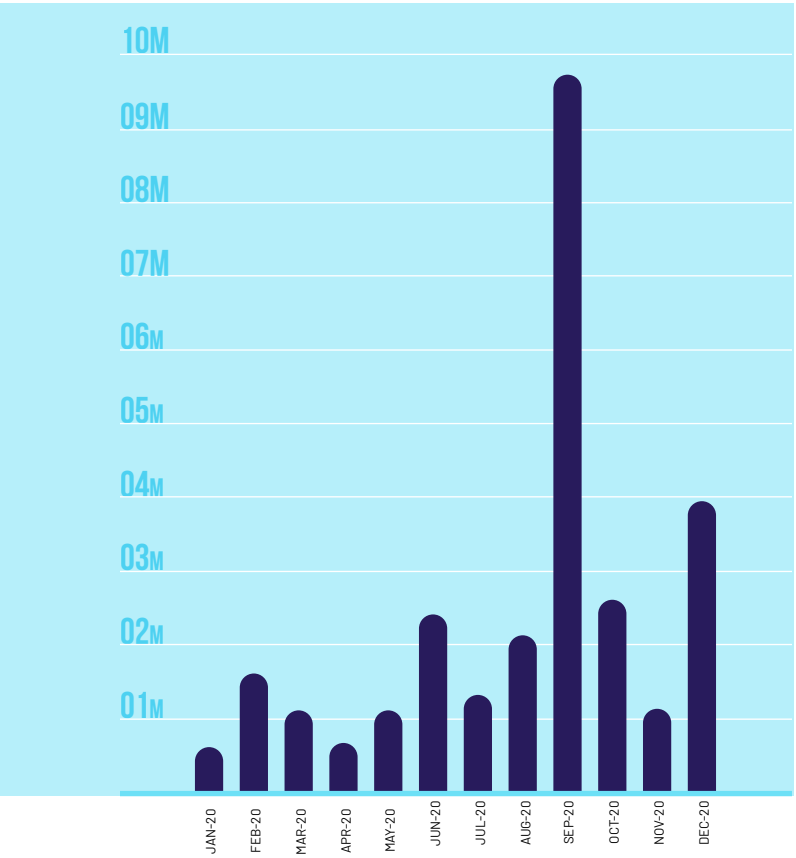
LESSON **05**

It's time to look at risk differently and stop finding excuses for why you can't manage that risk better.

Persistent threats from ransomware gangs, financial scammers, and hackers backed by nation-states are currently so prevalent we have devoted the third chapter in this book entirely to them—it's coming right up.

HEALTH CARE DATA BREACHES IN 2020

The number of people affected by breaches that were reported to HHS in 2020



Note: Data for December is incomplete because of a 60-day reporting window. Source: Department of Health and Human Services

[18] Ibid.

[19] Op cit. "Healthcare Industry To Spend $125 Billion."

"[All of] the logs and the graphs show, oh, man, these [attacks] have ramped up, it's hard to deny that," said Christopher Stroud, technology manager at Nebraska-based Great Plains Health. Stroud went on to say that Great Plains Health normally blocks around 10,000 attempts to access its servers every day—a number that tripled after it began coronavirus antibody drug trials, some days reaching 70,000 attempts or more.[18]

You just need to know where to look
(hint: it's not at your navel!)

WHAT YOU CAN DO TODAY

01 Start somewhere. Start anywhere. Start small and build toward a long-term goal. But start.

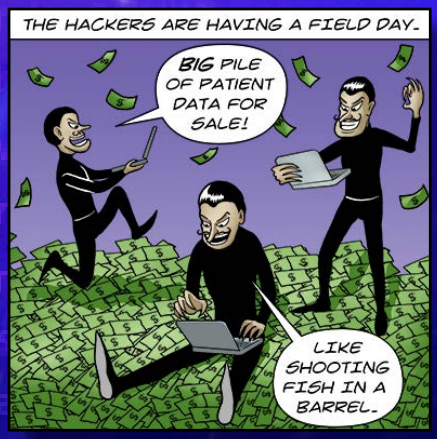
02 Choose a cybersecurity partner to help you navigate the sea of statistics and data and put a roadmap in place to better protect your HCO.

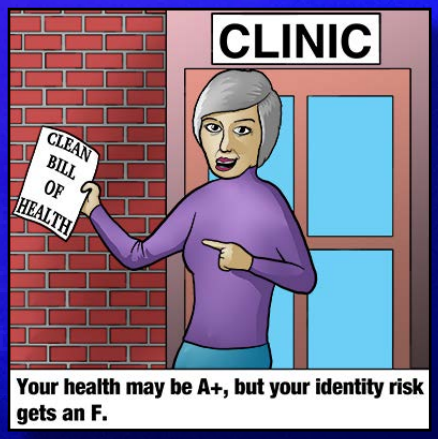
03 Look outside the healthcare sector to see where your peers in other industries have found success.

04 Make cyber protection a budgetary priority.

There will always be numbers to hold you back—even noted cybersecurity author Brian Krebs reported that hospitals hit by a data breach or ransomware attack can expect to see an increase in the death rate among heart patients in the following months or years because of cybersecurity remediation efforts[19]—but It's important to remember that **remediation after a breach is orders of magnitude more complex and costly than the ongoing fixes you can achieve with the right people, processes, and technology in place.** Keep reading to learn how.

CHPTR
03
DATA FOR RANSOM





UNF**KING CYBERSECURITY by CYVATAR.AI

LESSON 06

Ransomware isn't going away. Ignore it at your—and your patients'—peril.

If there's one common denominator across all HCOs—whether payor, provider, or OEM—it's risk. And risk from ransomware has been steadily rising in every major healthcare sector, not just because of data-rich PHI, but also because threat actors know that most HCOs are ill equipped to defend against it.

Cyber threats are four times more likely to be centered on healthcare than any other industry, and ransomware attacks are increasing in popularity because of the amount of privileged information a hacker can obtain.[21] For HCOs, the prospect of data being leaked on the internet is particularly disturbing, as it can involve sensitive private medical data alongside other forms of patient PII.

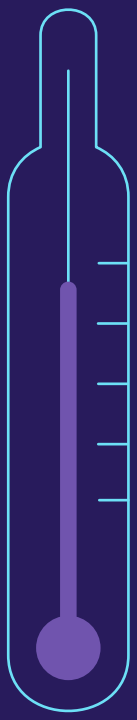
SPECIAL REPORT

CALIFORNIA

A medical clinic in Simi Valley, California, shut its doors after being infected by a ransomware attack

Sonoma Valley Hospital suffered a ransomware attack that impacted all of the hospital's computer systems; the hospital quickly stopped the incident by taking its electronic systems offline and didn't pay any ransom

Ascend Clinical was breached after an attacker deployed a successful phishing scheme that led to a ransomware attack; the data of over 77,000 individuals was compromised, but it was unclear whether the ransom was paid or not[20]



MICHIGAN

An ear, nose, throat (ENT) and hearing center in Battle Creek, Michigan, closed after a ransomware hack wiped out all of its files

GERMANY

A woman seeking emergency treatment for a life-threatening condition died after a ransomware attack crippled a nearby hospital in Duesseldorf, Germany, and forced her to obtain services from a more distant facility

[20] Data adapted from: Morgan. Steve. "Healthcare Industry To Spend $125 Billion On Cybersecurity From 2020 To 2025." Cybercrime Magazine. September 8, 2020;

Goodin, Dan. "Patient dies after ransomware attack reroutes her to remote hospital." Ars Technica. September 17, 2020; and

Webster, Ben. "Mitigating Healthcare Ransomware Attacks." Infosecurity Magazine. December 17, 2020.

[21] Ibid. "Healthcare organizations are sitting ducks."

As we discussed in the last chapter, hackers have also found it easy to attack hospitals with ransomware because of hospitals' rapid adoption of IT without a concomitant increase in the number and sophistication of IT support staff. Without adequate disaster recovery and backup plans, many HCOs are forced to pay the ransom. Additionally, the financial costs associated with business recovery after ransomware attacks are significant and growing.

PATIENT Pat

"What is Ransomware?"

Ransomware:

A type of malware that infects systems and files, rendering them inaccessible until a ransom is paid.[22] When this occurs in the healthcare industry, critical processes are slowed or become completely inoperable. HCOs are forced to go back to pen and paper, halting medical activities and ultimately soaking up funds that may otherwise have been allocated to upgrading or modernizing facilities.

Opportunistic Ransomware:

These campaigns employ spray-and-pray tactics, propagated through user-initiated actions such as clicking on a malicious link in an email, visiting a compromised website, or using malvertising. A few variants of opportunistic ransomware are also spread using server message block. However, an initially opportunistic tactic, such as a victim opening a wide-spread malicious email attachment, could turn into a strategic campaign if the call to action (CTA) takes further steps based on the target.

Strategic Ransomware:

These campaigns occur when a victim is specifically targeted or the threat actors realize that a sensitive entity has been reached through opportunistic methods. After a network compromise, CTAs will map the network to ensure the most critical data is identified and targeted during the ransomware encryption process. During this initial infection phase, CTAs seek to escalate privileges to an administrator or domain-controller level, while simultaneously identifying data backups so that the victim cannot easily regain control of the network or restore their files once the data is locked or encrypted. Ransom amounts often vary based on the CTA's assessment of the victim's network and data, in addition to the target's ability and need to pay.

[22] Definitions and types of ransomware adapted from the Center for Internet Security. "Ransomware: In the Healthcare Sector."

Currently, almost half of all data breaches in hospitals and the wider healthcare sector are a result of ransomware attacks: **560 healthcare provider facilities fell victim to them in 2020 alone.** In fact, data show a 45 percent increase in attacks on the healthcare sector for 2020 versus less than half this figure (22 percent) for all other verticals.[23]

We know outdated systems and insufficient cyber defenses play a role in the dramatic rise in ransomware attacks, but bad actors are also adept at launching attacks across multiple attack vectors. Email phishing campaigns, software vulnerabilities, and remote desktop protocols are the top three vectors used to launch these pervasive attacks.

For large organizations with lots of employees, human resources (HR) systems provide an additional attack vector that allow bad actors to steal the PII of employees as well as patient PHI and sell it online to the highest bidder; access to HR systems also makes it easy for hackers to use employee information to conduct sophisticated phishing attacks from inside the HCO itself.

Such ever-evolving threat variants and techniques make it hard for security experts to keep up, while platforms such as ransomware as a service (RaaS) make it easy for anyone—even malicious actors with little to no technical skill—to launch ransomware attacks against their victims of choice. A number of threat actors are known to auction data or to invite offers from interested third parties, while others may contract to other governments or even be in their direct employ.

"It's been months since the ransomware attack on my local hospital, and I don't know if my health information was stolen or not. I changed my username and password in the patient portal, and I got free identity theft protection, but Icriminals might have my home address or credit card."

PATIENT *Pat*

[23] Muncaster, Phil. "Ransomware Surge Drives 45% Increase in Healthcare Cyber-Attacks." Infosecurity Magazine. January 5, 2021.

When a ransomware attack is successful, the damage to patient care, IT resources, and recovery costs to systems already strained by COVID-19 can be devastating. In 2020, such incidents caused ambulances to be rerouted, radiation treatments for cancer patients to be delayed, medical records to be rendered temporarily inaccessible (and in some cases, permanently lost), while hundreds of staff were furloughed as a result of COVID-related disruptions.

The attack on the University of Vermont Health Network illustrates the fallout. UVM was forced to operate under EHR downtime procedures for more than a month; its patient portal, EHR, and lab results were largely inaccessible during that time.

Estimates show the attack cost UVM about $1.5 million a day in increased expenses and lost revenue, not including costs related to recovering its systems post-attack. The total cost could reach $63 million or more.

Other attack vectors include threats to medical devices, which have an average of 6.2 vulnerabilities each.[24] Another key entry point that allowed ransomware gangs to gain access to hospital networks was through a pair of VPN vulnerabilities. By the beginning of 2020, both vulnerabilities had been issued security patches to stop hackers from exploiting them,[25] but even as of this writing, many HCOs have yet to apply the patch.

CISOS SPEAK

"I've spent the bulk of my career as a CISO for health-care organizations, and one of the many things that makes cybersecurity a challenge for HCOs is the vast number of sub-verticals that comprise the healthcare sector. Compliance requirements differ greatly between, say, pharmaceutical or biotech orgs and the payers and providers for whom HIPAA and other regs loom large.

Smaller medical practices can't afford to keep pace with technological advances in security; most don't have CISOs or even dedicated security resources and rely instead on outsourced providers that often do not have the equivalent healthcare and security chops necessary to protect patient data adequately. Even larger organizations struggle with out-of-date tools and systems, making it complex and difficult for them to take advantage of the best solutions and resources available.

These varying degrees of threats, in addition to human vulnerabilities, sound like the perfect playground for cyber criminals. The trusting and empathetic nature of healthcare workers and the wildly different levels of digital and IT maturity of healthcare organizations combined seems like a mul-timillion-dollar mansion with the doors and windows wide open...and all the valuables in full view."

JERRY STO TOMAS

CISO and functional CIO,
Healthedge Software

[24] Op cit. "Healthcare Industry To Spend $125 Billion." Last year, 60 percent of medical devices were at end-of-life stage, with no patches or upgrades available.

[25] Palmer, Danny. "Ransomware attacks now to blame for half of healthcare data breaches." ZD Net. January 15, 2021.

Additionally, multiple hospitals across the U.S. were recently infected with ransomware using outdated JBoss server software. In these cases, threat actors uploaded malware to the out-of-date server without any interaction from the victim. Hollywood Presbyterian Hospital in California was one of the hospitals affected, in a case which delayed patient care and ultimately resulted in the hospital paying $17,000 to regain network and file access.

And then there's the pandemic. **Hackers continue to exploit vulnerabilities stemming from COVID-19, resulting in a 667 percent increase in phishing attacks.**[26]

Financially motivated cyber criminals have increased their targets in the healthcare sector since the start of the COVID-19 crisis, well aware that hospitals and clinics would be distracted with the huge surge in COVID cases coming through their doors. These groups are increasingly using APT-style tactics to gain a foothold in networks, perform lateral movement and credential theft, and exfiltrate data before deploying their ransomware payload. The use of Ryuk ransomware emphasizes the trend of having more targeted and tailored ransomware attacks rather than using a massive spam campaign, allowing attackers to ensure they hit the most critical parts of the organization to boost their chances of getting the ransom paid.

Unfortunately, these hacks show no sign of abating: **ransomware attacks on healthcare organizations predicted to grow fivefold by the end of 2021,**[27] **driven in part by more patients using remote care but also because the industry's response to ransomware attacks has spurred cyber criminals on. The willingness of hospitals and physician practices to pay high ransoms to regain their data quickly motivates hackers to keep their focus on patient records.**[28]

LESSON 07

Not all attacks use targeted or sophisticated techniques. Attacks modeled on advanced persistent threats (APTs) can lurk inside systems for days, months, and even years before crippling healthcare operations.

[26] Op cit. "Mitigating Healthcare Ransomware."

[27] Op cit. "Healthcare Industry to Spend 125 Billion."

[28] https://www.infosecurity-magazine.com/news/healthcare-data-breaches-to-triple/

WHAT YOU CAN DO TODAY[29]

01 Create an incident response plan that includes what your organization should do during a ransomware event.

02 Use tableop exercises to prepare your team for the expected and unexpected ransom attacks.

03 Perform regular system backups and routinely test those backups for data integrity.

04 Store back-ups offline when possible.

05 Apply additional controls, such as IP whitelisting or MFA, wherever you can.[30]

06 Filter email and inbound and outbound network traffic based on IP addresses; use geographic and threat-based blocking to minimize the attack surface.

07 Provide training to help users identify suspicious emails or links and ensure they are aware of the dangers of opening unsolicited emails.

08 Create policies regarding suspicious emails so they can be reported effectively.

09 If remote access is required by a third-party vendor, develop protocols that keep user accounts disabled until access is required.

10 Remove unsupported legacy systems where possible and purchase extended support for older systems that are critical to your operations if available.

It is important to understand that cyber attacks are inevitable because nefarious agents are always finding new ways to exploit vulnerabilities. Strong password policies coupled with MFA can significantly improve security. And by **combining risk controls with employee training, you will be better positioned to stay ahead of bad actors.**

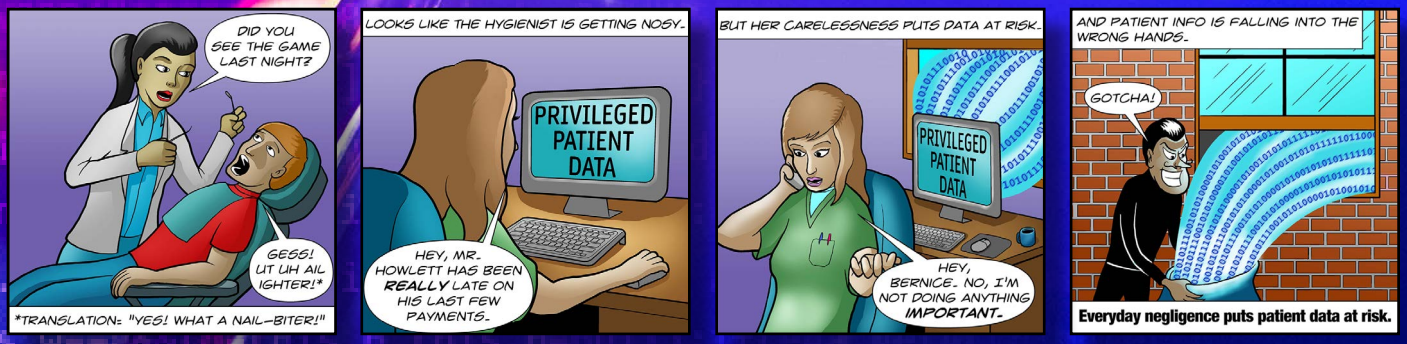
[29] Some of these are widely known, common-sense-based suggestions; others are adapted from the Center for Internet Security. "Security Primer—Ransomware."

[30] Op cit. "Mitigating Healthcare Ransomware." MFA requires users to verify their identities with different forms of authentication—a layered approach that fortifies healthcare organizations against attacks during login and password reset attempts.

CHPTR

04

IS YOUR FRONT OFFICE LEAVING A BACK DOOR OPEN?



UNF**KING CYBERSECURITY by CYVATAR.AI

As we've discussed, HCOs fall victim to data breaches more than any other industry at the alarming rate of nearly 45 percent. **On average, it takes about 350 days to identify and contain a healthcare-related data breach**—that's almost an entire year of exposed data and unpatched vulnerabilities during which more damage can occur.

LESSON 08

Insider breach remediation alone can cost upwards of $10 million annually, and that's just for people who work with or for your organization!

Ten million dollars is a big enough number for us to devote some ink in an effort to understand the nature of insider hacks and what you can do to prevent them.

LESSON 09

With more personnel working and connecting remotely, the traditional walls have become more porous than ever, and increased attention needs to be paid inside.

By some estimates, more than half of insider fraud incidents in healthcare involve the theft of customer data.[31] The 2019 Verizon Insider Threat Report (ITR) found that **46 percent of healthcare organizations were affected by insider threats—the only industry where insiders were responsible for a higher percentage of breaches than external actors.** In fact, year after year, insiders have been consistently named the biggest risk to healthcare data. The challenge is in protecting against passive, accidental threats and active, intentional threats at the same time.

[31] Op cit. "Healthcare Industry To Spend 125 Billion"

"What Makes Insiders so Dangerous?"

PATIENT Pat

Insiders pose a serious threat to businesses in nearly every industry, but the healthcare sector can be particularly prone to attacks from this flank because:

HCOs are a rich and easy target. As we've discussed, the treasure trove of PHI is far more valuable than simple credit card data or login credentials, because bad actors can gain complete profiles on the people whose information they steal—and that means attack vectors beyond just ransomware are in wide use. Social engineering scams like phishing and business email compromise are also employed in the pursuit of comprehensive patient information.

Human behavior in many healthcare sectors tends to be, well, human. When you're dealing with people who've been trained to help other people in crisis, to be open and empathetic, you're dealing with people who are much easier to social engineer, unlike their more seasoned (not to say cynical) counterparts in, say financial services or government agencies.

Educating frontline workers about cybersecurity is rife with challenges unique to the healthcare industry because:

- Most of them may be clinically proficient or technically inclined in the life sciences but are not necessarily computer savvy or technical in an IT capacity
- They're focused on helping patients, so building good cyber habits may feel like a distraction
- They're already stymied by outdated equipment and IoT advances they may not fully understand
- HIPAA took too long to facilitate digital records, which itself ushered in huge change-management complexities on top of all of the technical ones, making it difficult for health workers to find the time to learn new systems and still provide quality care
- Many HCOs employ tenured doctors or other workers with outsize veto power, making it easy for the established regime to resist necessary change

Insiders also pose a threat because the legitimate access they have (or had) to proprietary systems circumvents traditional cybersecurity defenses, such as intrusion detection devices or physical security. While an insider may be simply careless—by repeatedly violating policies, for example—others maliciously cause destruction by giving away access codes or purposely selling PHI for profit.[32] And with stolen and compromised credentials causing ongoing issues for 53 percent of health systems,[33] it's hardly an inconsequential concern.

Insider threats take many forms, and they can come from any part of an HCO's ecosystem, whether HR, Facilities, Billing, Administration, or partners. The five major insider threat profiles you need to know include:[34]

01 THE CARELESS WORKER.

The careless worker may be perfectly well-meaning, but their actions can carry significant privacy and legal implications when they bypass security or privacy measures. In 2018, healthcare organizations paid a record-breaking $28 million in financial penalties to the Office for Civil Rights (OCR) in response to HIPAA violations.

When employees break acceptable use policies, leave sensitive PHI in plain sight, forget to logout of terminals, or install unapproved applications on company devices, they leave their network vulnerable to infiltration and exploitation. Careless workers are usually unaware that they're committing violations even as they snoop on coworkers, peak at neighbor's records, or violate internal policy by self-accessing their own records because "everybody does it."

Such negligence makes careless workers every bit as dangerous as those with malicious intent. To prevent the careless worker from breaching patient data and putting your organization at risk, you can establish and reinforce guidelines from the point of hire. Patient privacy monitoring can also help you spot common trends in improper access and anomalous behaviors that can inform retraining and remediation efforts to create a culture of privacy.

02 THE INSIDE AGENT.

Inside agents could be anyone from the contract IT worker to the custodial staff to the head of the accounting team. Typically, the inside agent is an employee who has been coerced, recruited, or bribed into siphoning data from the HCO to a third party. HIPAA enables you to thwart inside agents by restricting file access to only authorized users; you can also implement user activity monitoring controls to send alerts when suspicious activity is detected to help reduce inside agent risk.

03 THE FECKLESS THIRD PARTY.

Feckless third parties are typically business associates that compromise security through improper use or harmful access. In January 2019, business associate breaches were responsible for more than 100,000 leaked patient records over a single month. To mitigate risks from feckless third parties, you can install a system that monitors suspicious network traffic, unusual activity, and remote access. These measures, along with disabling any compromised user accounts, can help protect against potential third-party vulnerabilities.

[32] Center for Internet Security. "Insider Threats: In the Healthcare Sector."

[33] Op cit. "Healthcare organizations are sitting ducks."

[34] Adapted from Imprivata. "5 Types of Insider Threats in Healthcare—and How to Mitigate Them." March 28, 2019.

04
THE DISGRUNTLED EMPLOYEE.

Whether they've been let go for missing quotas or are looking to transition to another company, the disgruntled employee is another potential threat. It's easy for folks in this group to feel as though they were treated unfairly, and if they are angry or in a financial bind, they may be tempted to leak PHI or take private data with them. They could also turn into an inside actor, vulnerable to criminal activity in their final days before termination or resignation. You can combat disgruntled employees by scanning for signs an employee is about to quit and restricting controls before they exit.

05
THE MALICIOUS INSIDER.

Malicious insiders are one of the most challenging threats to detect. Unlike the inside actor, they typically act from their own motivations rather than those of an external party. They can leverage their privileges to access private information for personal or financial gain, and because they're already inside the network, they have no roadblocks preventing them from abusing secure data—and they wouldn't hesitate to leak PHI for profit. To combat them, you can use countermeasures such as controlling access so that only individuals with a need to know can log in, programming screen locks, monitoring users for suspicious activity, restricting the use of USB storage devices, and disabling access for any inappropriate activity.

Cautionary Tale: An insider victimized one Texas hospital when he used the hospital network to build a botnet to attack rival hacking groups. The individual—a night security guard—was caught after he filmed himself staging an infiltration of the hospital network and then posted it on YouTube. The investigation revealed that the security guard had downloaded malware on dozens of machines, including nursing stations with patient records. He also installed a backdoor in the HVAC unit, which could have caused damage to life-saving medications. The guard's folly landed him big fines and nearly a decade in prison—but spared the hospital significant fallout because he posted his exploits on social media.

"We're seeing a lot of insider threats, unfortunately, where folks may recognize that their systems aren't patched as strongly as they should be or completely as they should be, and they're able to just insert this software right into some unsecured systems. One of the biggest examples we've actually seen recently is with the UHS health care system where computers were infected, and many practices had to shut down."[35]

Laura Hoffman
AMA Assistant Director of Federal Affairs

[35] Drees, Jackie. "Beware of insider cyber threats, AMA warns hospitals." Becker's IT Health. December 1, 2020.

PATIENT Pat

"I wash my hands and wear a mask to boost my personal hygiene. What's my provider doing to bring cyber hygiene to my data?"

Meanwhile, the COVID pandemic led to an explosion of phishing scams, further widening insider threat risks, particularly from careless workers and feckless third parties. Many of the fake emails appeared to come from organizations such as the World Health Organization and the U.S. Center for Disease Control, tasking already overburdened IT and security teams to keep on top of them.

The most recent HIMSS Cybersecurity Survey pointedly notes that nearly 60% of hospital representatives and healthcare IT professionals said that email (including phishing scams) was the most common point of information compromise.[36]

Meanwhile, understaffed, underfunded IT and security departments are scrambling to accommodate the surge in demand of remote services from patients and physicians while simultaneously responding to increases in security risks,[37] and mandates regarding the portability of healthcare records adds yet another burden to their already stretched resources. And none of this includes the Department of Health and Human Services' enforcement discretion to a number of data sharing circumstances, including telehealth exceptions, public health entities, temporary COVID-19 care sites, first responders, and the like, further compounding the need to balance transparency with the increase in data sharing.

HCOs can boost consistent cyber hygiene and habits—particularly to help staff work through emails and suspect URLs—as the equivalent of proper hand washing.

LESSON 10

HCOs continue to struggle to meet the needs of data not being accessed outside of approved channels and partners and in authenticating the data sets throughout their entire lifecycle, because the handoff from the original source must be able to be authenticated at any stage.

Fifty-nine percent of health system CIOs surveyed are shifting security strategies to address user authentication and access to make it harder for malicious incidents and hackers to gain a foothold in their health systems,[38] in part to combat the 90 percent of healthcare employees who shifted to working

[36] Ibid.

[37] Op cit. "Healthcare organizations are sitting ducks."

[38] Ibid.

at home as a result of the pandemic but did not receive any guidelines or training to help them combat the risk to sensitive patient data or systems. In fact, **nearly a third of U.S. health employees have never received cybersecurity awareness training at all,[39] a number that exceeds 40 percent for clinical hospital employees.[40]**

When one inadvertent click can jeopardize patient safety, evolving defensive practices is critical.

WHAT YOU CAN DO TODAY

Fortunately, insider threats can be reduced using a variety of easy-to-implement measures:

01 Launch a thorough HR process that includes onboarding, security education, disciplinary action, and exit procedures.

02 Establish ongoing compliance training.

03 Ban weak and compromised passwords and enforce stronger password policies. Instead of requiring all users to change their passwords at the same time, length-based aging allows more granular control by forcing expiriations less frequently for users with stronger passwords.

04 Provide security awareness training to help users identify threats such as phishing and social engineering attempts and define steps employees can take when something seems suspicious.

05 Perform network segmentation and apply access controls between each segment.

06 Ensure users have only the minimum level of access required to accomplish their duties.

07 Never allow reuse of the same credentials across multiple accounts, systems, or terminals.

08 Regularly review vendor accounts and their associated passwords to ensure they have been changed from default settings.

Training your users and employees how to recognize and report an insider threat (or prevent them from inadvertently becoming one) is an excellent first step toward protecting your organization. There are many training programs and educational materials that cover explanations on what suspicious activity looks like and the kinds of behavioral changes employees should be looking for in their colleagues—and where to go for help if they find any.

[39] Op cit. "Healthcare Industry To Spend $125 Billion."

[40] Op cit. "Healthcare organizations are sitting ducks."

CHPTR
05

HIPAA AND HITECH AND HITRUST, OH MY!

UNF**KING CYBERSECURITY by CYVATAR.AI

We've said this many, many times, but it bears repeating:

LESSON 11 **Compliance is the byproduct of a strong security posture—not the other way around.**

Data privacy is critically important to healthcare organizations, and safeguarding PHI is often a matter of complying with legal and regulatory requirements as much as it is a security concern. For many organizations, navigating between the two can seem like being forced to choose between Scylla and Charybdis, but we'll show you in this chapter how you can have both without sacrificing the requirements of either one.

Maybe you're too small an organization to have set aside budget dollars for cyber solutions or maybe you feel forced to prioritize compliance requirements over security investments. These are situations we see every day. It's not at all uncommon for healthcare executives to find themselves without the time to understand security or to lack the staff required to focus on it. Security functionality often gets bumped, especially in development, in favor of the features and capabilities explicitly addressed to patient safety.

And they're not alone.

61 percent of corporate board members across industries admit they would compromise on cybersecurity in order to achieve a business objective.[41]

The downside is of course that only 16 percent of executive leaders say their companies are well prepared to deal with cyber risk. A recent McKinsey report notes that growth in most industries depends on new technology, such as artificial intelligence, advanced analytics, and the Internet of Things (IoT), which may expose companies to new types of cyber risk from new or evolving threat vectors[42]—a scenario HCOs know only too well.

To bridge the gap, you may decide to beef up on compliance. However, **healthcare organizations, like other companies, invest in compliance activities to follow various laws and regulations—not necessarily to improve their security posture.**

Healthcare is rife with regulatory requirements. Understanding how different frameworks intersect with cybersecurity resilience—and how you can successfully support both—is paramount.

HIPAA[43]

Perhaps the most well-known term in the bunch, the Health Insurance Portability and Accountability Act (HIPAA) protects workers from losing health insurance if they lose or change jobs and helps ensure the privacy and security of PHI. It also attempts to standardize the methods by which HCOs store and exchange sensitive information.

[41] National Association of Corporate Directors. "Business Model Disruptions, Slowing Global Economy Top List of Corporate Directors' Concerns For 2020." Globe Newswire. December 11, 2019.

[42] McKinsey & Company. "Perspectives on Transforming Cybersecurity." March 2019.

[43] Adapted from Pruitt, Gina B. "Part 1: What the H?" Nashville Medical News Blog. June 8, 2017.

"Every time I visit my doctor, I sign more documents around the use of my personal information. It's so confusing! I have no way of knowing what happens to that information when I provide it. Like everyone else, I quickly sign the forms even if I don't fully understand them."

PATIENT *Pat*

The Security Rule: Provides the administrative and technical requirements that HCOs must meet to ensure the confidentiality and security of PHI. Under the Security Rule, HCOs must assess their own potential for risks to PHI and take "reasonable and appropriate" measures to secure systems and processes. At minimum, such security might include data encryption.

The Privacy Rule: Provides rights to individuals (and grants some permissions to HCOs for use of PHI for specified purposes). If HCOs would like to disclose consumer health information for purposes that are not explicitly permitted by the Privacy Rule, the consumer must first give written permission. HCOs then must specifically tell the consumer how they plan to use that information.

The main requirement for HIPAA compliance is an annual risk analysis, but for all the rest of the year, you may be out of compliance. Or worse—you could be vulnerable to a breach.

HITECH[44]

HITECH, or the Health Information Technology for Economic and Clinical Health Act, operates as an updated extension of HIPAA. **Where HIPAA built the structure for regulation of health information technology, HITECH provides more details and increased enforcement for HIPAA violations.**

HITECH also extends HIPAA's stipulations to business associates, so any organization that has access to PHI must also be HIPAA-compliant. Whereas enforcement of HIPAA was previously perceived as somewhat lax or inconsistent, HITECH institutes steep penalties for willful neglect—and mandates audits by HHS.

With the implementation of HITECH, HCOs are required to notify individuals when their information has been breached; they must also notify both the HHS and local media when the breach affects more than 500 patients.

[44] Ibid.

HITRUST[45]

Unlike HIPAA and HITECH, the Health Information Trust Alliance (HITRUST) is not a law. It is a private organization of providers and payers that created a certifiable framework for healthcare technology security, designed to ensure compliance with HIPAA and other existing security frameworks.

HITRUST works to harmonize the various regulatory standards and frameworks set up by federal agencies; it gathers information from HIPAA, HITECH, NIST, ISO, COBIT, and PCI to create a standardized view of information security and privacy needs.[46] HITRUST also attempts to provide HCOs a path to compliance, governance, and risk management including certification processes that cover existing security regulations for the handling, storing, and transmission of PHI. But the certification process is lengthy—it can take anywhere from 12 to 24 months—and HCOs that complete the certification process must recertify every two years.

The time and costs associated with HITRUST can be steep for smaller organizations without the staff or resources to keep up. **And remember—there are no direct legal repercussions related to HITRUST; it just becomes another checkbox in a vast sea of compliance boxes to check—none of which makes your data or your patients any more secure. Additionally, using the HITRUST CSF does not provide you with even a certificate of HIPAA compliance.**

Steep fines, hidden costs, jail time, and reputational damage are certainly serious consequences of noncompliance or violations. But it's important to remember the primary purpose of security and privacy measures is to protect your patients.

LESSON 12

If you have access to PHI, it's your responsibility to secure their personal information for their safety—and not just because you'll get fined if you don't.

"Why are there so many IT and cybersecurity standards and why do they seem so complicated and contradictory? Who's really in charge of keeping my PHI safe?"

PATIENT Pat

[45] Ibid.

[46] Goddard, Robert. "HIPAA vs. HITRUST: What are the Differences?" IS Partners. July 30, 2020.

HCOs should assign at least one person to oversee their compliance program, someone responsible for ensuring the entire organization adheres to both its external regulatory requirements and its internal policies. While most large HCOs have a designated compliance officer, smaller ones do not—but outside security expertise on demand can help meet this need.

A poll of 3,500 healthcare consumers that used medical or hospital services in the last 18 months revealed 93% would leave their provider if their patient privacy was compromised in an attack that could have been prevented.

LESSON 13

MANAGING RISK

HIPAA requires HCOs to analyze the specific risks and possible vulnerabilities their organizations face; they must also take "reasonable and appropriate" measures (i.e., the implementation of security and privacy controls) to eliminate potential risks to PHI:[47]

01 **You must know where PHI is stored within your system and how it is being created, received, and transmitted.**

02 **You're also responsible for how your affiliated businesses handle PHI because they must be HIPAA compliant as well.**

03 **You should be aware of every server, computer, device, application, filing cabinet, and email that comes into contact with PHI.**

04 **You must test your security controls and identify specific threats to your systems.**

05 **Are you using operating systems or software that can be easily hacked?**

06 **Have you encrypted ALL devices (not just computers) that handle PHI?**

07 **Is data encrypted in transit, at rest and when stored (e.g., including backups and external drives)?**

08 **Know who in your organization has access to PHI: Do they have a business need for such access? Then ensure that those with access are appropriately trained on HIPAA.**

09 **Are you properly terminating access and credentials for ALL former employees and business affiliates at or prior to termination?**

10 **Though it's not explicitly required by HIPAA, vulnerability scans and penetration testing are effective methods for identifying risks that need to be mitigated.**

[47] Adapted from Pruitt, Gina B. "Part 2: How the H?" Nashville Medical News Blog. June 19, 2017.

Patient push-back bolsters the need for internal—or external—security expertise that can successfully advocate for improved cyber resiliency. As one researcher remarked, "Medical and financial leaders have wielded more influence over organizational budgets and made it difficult for IT management to implement needed cybersecurity practices despite the existing environment, but now consumers are beginning to react negatively to the provider's lack of protection solutions."[48]

Unfortunately, multiple regulatory requirements force organizations to meet compliance challenges that often compete with each other. Furthermore, all of them require constant monitoring, frequent audits, and professional staff and technologies, which drives up the cost to stay in compliance.[49]

As a result, many companies tend to decouple compliance requirements from their security strategy, **putting these two critical safeguards in competition with each other and nearly always sacrificing a strong security posture in favor of fulfilling compliance needs.** Compliance becomes the entire security strategy.

Additionally, the consequences of non-compliance can be costly. Business disruption represents the most expensive consequence of compliance failure, followed by fines, penalties, and other settlement costs:[50]

REAL DATA

TIER	TYPE OF OFFENSE	MINIMUM FINE	MAXIMUM FINE
01	Unaware of violation; could not have realistically avoided	$100+ per violation, up to $50,000	$1,500,000 per year
02	Should have been aware of the violation; could not have avoided (not quite willful neglect)	$1,000+ per violation, up to $50,000	$1,500,000 per year
03	Occurred due to willful neglect; attempt made to correct the violation	$10,000+ per violation, up to $50,000	$1,500,000 per year
04	Occurred due to willful neglect; no attempt made to correct the violation	$50,000+ per violation	$1,500,000 per year

In addition to the federal fines, consider other potential costs that a HIPAA violation could mean for your practice or facility. You could lose many business hours trying to settle the situation, and you'll likely incur hefty legal fees as well.

[48] Ibid. "Healthcare organizations are sitting ducks."

[49] Ponemon Institute. "The True Cost of Compliance with Data Protection Regulations." December 2016.

[50] Adapted from Pruitt, Gina B. "Part 3: Why the H?" Nashville Medical News Blog. June 29, 2017.

TIER	DESCRIPTION OF VIOLATION	JAIL SENTENCE	FINE
01	Obtaining PHI for reasonable cause or having no knowledge of violation	up to 1 YEAR	up to $50,000
02	Obtaining PHI under false pretenses	up to 5 YEARS	up to $100,000
03	Obtaining PHI for personal gain or malicious purposes	up to 10 YEARS	up to $250,000

REAL DATA

Notable criminal HIPAA prosecutions include:

- Huping Zhou, a former researcher at UCLA Medical Center, became the first person sentenced to jail time for a HIPAA violation. He received four months of jail time, a year of supervised release, and a $2,000 fine for reading private medical records—including those of celebrities and his co-workers. According to U.S. District Attorney's Office Spokesman Thom Mrozek, **Zhou was also the first person to be convicted and sentenced for a violation even though he did not sell or improperly use the information. In fact, Zhou claims that he was not even aware that his actions constituted a crime**—but of course ignorance of the law is no excuse.
- Denetria Barnes, a nursing assistant at an assisted living facility in Florida, and her boyfriend obtained and attempted to sell PHI for personal gain. **Denetria was sentenced to 37 months in prison and three years of supervised release;** she is now barred from working in any job where she has access to people's identification information.
- **Helene Michel, the former owner of a medical supply company in New York, was convicted of not only criminal HIPAA violations, but also $10.7 million in Medicare fraud.** She was sentenced to 12 years in prison—one of the harshest HIPAA-related sentences yet.
- **Joshua Hippler, an employee of a hospital in Texas, obtained PHI that he intended to use for personal gain: He was sentenced to 18 months in prison.**
- Premera Blue Cross settled potential violations of HIPAA Rules and paid a $6.9 million penalty; Excellus Health Plan settled for slightly less, at $5 million.[51]

Unfortunately, in addition to identifying vulnerabilities within your organization, you are also responsible for assessing the severity of each threat, which is virtually impossible to do effectively without remediation capabilities. And remediation is part of your security strategy. It puts the teeth in your compliance efforts and gives you real tools to stave off cyber threats.

[51] Adapted from Pruitt, Gina B. "Part 3: Why the H?" Nashville Medical News Blog. June 29, 2017.

In the meantime, security itself becomes an afterthought, an add-on to organizational goals, rather than a critical, integral part of them, making it impossible for security to act as a catalyst for healthy growth.

The add-on approach may even become a drag on business velocity by increasing user friction or delaying time to market for new product features. When secure systems are not usable, there is a risk that users may try to avoid them or disable the security features entirely. As one CISO put it, "If you build an overly burdensome solution, users will do their best to circumvent it."

LESSON 14 | **Done right, compliance simply becomes the byproduct of a sound security strategy.**

WHAT YOU CAN DO TODAY

01 Always approach security as an integrated exercise that spans all of your business goals—including compliance.

02 Never force yourself to choose between security and compliance—you can easily have both by focusing on a long-term security roadmap; compliance is a byproduct of good security.

03 Complete a readiness assessment. You should review your current control environment to identify gaps between current controls and what you need to ensure cyber resilience.

04 Before joining a new practice, ask about existing security protocols—have they been breached? What action have they taken to protect patient data?

Remember, a successful, integrated security strategy will deliver the compliance requirements you need and support a public-facing security stance that builds inherent trust with patients and consumers, leading to long-term growth and increased security confidence.

CHPTR
06

MANAGED SERVICES PROVIDERS LEAVE YOU HOLDING THE BAG

UNF**KING CYBERSECURITY by CYVATAR.AI

In today's complex healthcare environment, the reliance on collaborative partnerships is key to success. 2019 saw a 153 percent increase in the number of reported state, local, tribal, and territorial (SLTT) government ransomware attacks from the previous year, largely attributed to Ryuk ransomware infections and compromises affecting managed service providers (MSP) that service them.[52]

LESSON 15

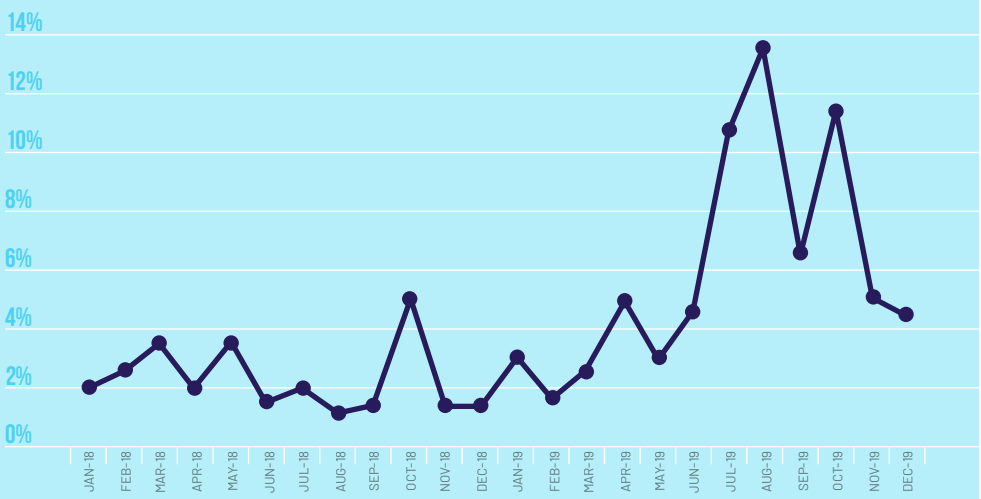
Cybersecurity may be a new(ish) line item for HCOs, yet many budgets have not evolved to cover the true cost of people and technology requirements.[53]

Recently, heightened awareness around cyber threats and the shift of CISOs reporting up to the C-suite have helped put more of a spotlight on cybersecurity budgets, but many small medical offices have not yet reached the point where security is prioritized as part of overall patient safety.

The shortage of healthcare cybersecurity professionals in turn fosters rapid spend to acquire technology and services to bridge the gap. Nevertheless, **51 percent of in-house IT leaders report their group is not aware of the full variety of cybersecurity solutions that exist,** particularly mobile security environments, intrusion detection, attack prevention, forensics, and testing in various healthcare settings.[54]

SLTT RANSOMEWARE INCIDENTS

The percentage of SLTT incidents by month during 2018–2019.



Source: Victim Disclosure, 3rd Party Disclosure, Open Source

[52] Op cit. "Security Primer—Ransomware."

[53] Op cit. "Healthcare organizations are sitting ducks."

[54] Ibid.

We often hear of "shared-risk" arrangements, "value-based" care, and "accountable" care organizations, all of which are designed for better patient outcomes. So **why hasn't the healthcare industry demanded these types of approaches from security vendors?**

Enter the MSP.

Managed services providers (MSPs), like their managed security services provider (MSSP) counterparts, may purport to help HCOs sift through the deluge of technology and security products available, implement new solutions, or assess existing investments, but these engagements can be costly relative to results, and all too often you're the one who'll be left holding the bag when the partnership fails to produce the promised outcomes.

The failure of MSPs to live up to their promise lies chiefly in two areas: their lack of cybersecurity expertise and their inability to integrate into the entirety of HCO IT environments.

MSPs have plenty of staff with IT skills, but when it comes to selecting and installing security solutions, rather than choosing tools best suited to your unique requirements, they're likely to sell what they know or have heard about, making it difficult to integrate fully—let alone easily or seamlessly—into your environment. Any SaaS-based or non-traditional solutions you may have previously purchased pose additional integration challenges if they are to fall within the MSP's scope of work.

The disparity among various investments ought to be addressed in the MSP (or MSSP) agreement, but that's rarely the case. You're more likely to believe the MSP is responsible for managing all of the security and technology solutions you own in addition to anything new they introduce, but if the MSP is incapable of supporting or integrating existing tools, visibility and coverage gaps will leave you more vulnerable to cyber threats than you were before the engagement.

Without continuous visibility and regular patching across the entire security environment, any incidents "discovered" by the MSP are likely to yield a high number of false-positives, the investigation and remediation of which then falls to you to resolve:[55]

99% of cybersecurity professionals say high alert volumes cause problems for staff

70% say the volume of alerts has more than doubled since 2015

85% struggle to cope with the near-constant barrage of such alerts

83% say their teams experience alert fatigue

Many providers deliver just such a barrage of security alerts, which is the equivalent of telling you your house is on fire. They shout! They point! They incite panic! You look wildly to them for help, but their buckets hold no water. Importantly, nothing in their services agreement holds them accountable for preventing your house from catching fire in the first place.

CISOS SPEAK

"Like lots of other organizations, we use managed services providers and managed security service providers to help us keep our systems and data secure, to lock out the bad actors, and lock down the controls necessary to keep patient information safe. We pay for these services largely on a contractual retainer-type basis, with the expectation that providers will be able to quickly and efficiently shift from business-as-usual operations to all-hands-on-deck when circumstances require it.

But it doesn't always work out that way. Sometimes, we're overburdened with alerts warning of malicious or suspicious traffic we have to investigate. Uncovering and dispositioning false positives takes us away from other important duties. Sometimes, providers use their own solutions or products from other vendors, making it difficult for them to work effectively in unique hospital environments—like when a breach occurs and they have no ability to access the right file logs on the fly to prevent the breach from taking hold and compromising other systems. That's a big problem.

We've also struggled with getting clear service levels for incident response (IR) services; some vendors charge additional fees for IR because they consider responding to an incident as activity outside the normal course of operations. But for us, swift, timely, effective IR is paramount. We hope to prevent hackers from gaining entry, but if they make it past our defenses we need to know our MSP will respond quickly to eradicate the threat."

AARON DESPAIN

Chief Information Security Officer, Hoag Memorial Hospital

[55] Data adapted from Scroxton, Alex. "Majority of security pros fed up with alert fatigue." Computer Weekly. July 9, 2020.

It's possible your provider will recommend some type of automated solution that delivers real-time incident analysis, but "analysis" is just a fancy word for alerts with context; it will not prevent or remediate an attack. Your house will still be a pile of ash, and you will still have to pay someone to clean it up and rebuild it.

LESSON 16

Most MSPs put the burden of incident investigation, prioritization, and remediation on you—a burden no HCO without a sound understanding of security, a solid process roadmap, and technically skilled resources is truly equipped to handle.

Never forget that, pre- or post-breach, all of the solutions in your security environment need to be managed and maintained continuously. The recent supply-chain ransomware attack that exploited a vulnerability in Kaseya software (which powered a central console for managing a wide range of IT operations) exposed just how attractive—and assailable—MSPs are across today's threat landscape.

To achieve the outcomes you expect and need with MSPs, MSSPs, or partners will require heavy lifting from you and your organization, either heading into the engagement, throughout it, or both.

WHAT YOU CAN DO TODAY

01 Don't be afraid to hold your MSPs and MSSPs to account by challenging them to prevent attacks before threats can execute inside your HCO.

02 Ensure they're obligated to assist in data recovery and remediation efforts if what they sell you fails.

03 Expect them to follow FBI and CISA guidelines that include the enforced use of multifactor authentication (MFA) on every internal account and as many customer-facing services as possible; the implementation of allowlisting to limit communication with remote monitoring and management (RMM) capabilities; and the placement of administrative interfaces of RMM behind a virtual private network (VPN) or a firewall on a dedicated administrative network.

Adopting principles of least privilege on critical accounts and maintaining the security basics covered in this book will go a long way toward keeping your HCO secure even from threats that originate at the MSP itself.

CHPTR
07

PEN TESTS AND LONG POCS STILL GET YOU BREACHED

UNF**KING CYBERSECURITY by CYVATAR.AI

Just like a doctor taking your temperature to see if you have a fever, traditional penetration tests only reflect the state of a security environment at a specific point in time.

They are not designed to anticipate future behaviors or predict likely outcomes. In fact, given the rapid pace of change and the dynamic fluidity of evolving threat vectors, a pen test won't give you much more than any other assessment tool, leaving you with vulnerabilities you have to find a way to remediate.

Software updates and new releases happen frequently—multiple times a day for companies that are heavily DevOps-oriented and many times a year for less sophisticated organizations[56]—making it impossible for a pen test to accurately reflect threats and vulnerabilities in an HCO at any time other than when the test itself is administered.

"What is a penetration test?"

PATIENT *Pat*

A penetration test, colloquially known as a pen test, pentest, or ethical hacking, is an authorized, simulated cyber attack on a computer system, performed to evaluate system security. The test is used to identify weaknesses such as the potential for unauthorized parties to gain access to private features and data.

Pen tests can help identify a system's vulnerabilities to attack and estimate how vulnerable it is. Targets may be a white box (about which background and system information are provided in advance to the tester), a black box (about which only basic information—if any–other than the company name is provided), or a gray box (a combination of the two where limited knowledge of the target is shared with the auditor). Penetration test reports may also assess potential impacts to the organization and suggest countermeasures to reduce the risk. Security issues that the penetration test uncovers should be reported to the system owner.[57]

[56] Wang, Dr Chenxi. "Pentest as a Service Impact Report: 2020." Cobalt.io.

[57] Adapted from Wikipedia

The truth is, an absence of business context has plagued pen test activity for a long time. The lack of knowledge about a particular type of customer or operating environment leads to the reporting of factors that often do not pose a genuine risk. The many sectors and subsectors in the healthcare industry and the wide diversity of their operating conditions compound the issue further.

Add to which, the effort associated with remediating vulnerabilities and closing gaps will almost certainly fall to HCO staff, after the pen test team has gone. To keep yourself protected, you can establish (or improve) your vulnerability management processes. Many HCOs have vulnerability scanning tools, but none can keep up with remediation needs. Even the largest organizations can't keep up with continuous vulnerabilities, so it might make sense to outsource security remediation to a firm that can be held accountable to improved outcomes. Once vulnerability management is established in the HCO, a pen test can help identify potential cyber risks and prioritize the remediation efforts required to minimize them—but if you don't have a plan in place to fix what you find, the pen test will be of little use.

The likelihood that you will find yourself wasting time trying to fix outdated issues with old approaches is high and could be costly, without making your HCO safer or more resilient.

Similarly, a proof-of-concept engagement (POC) often launches to help buyers understand the true results they can expect to receive from a product they have not yet purchased.

"What's a POC?"

PATIENT Pat

Proof of concept (POC), also known as proof of principle, is an application of a certain method or idea in order to demonstrate its feasibility, or to verify that some concept or theory has practical potential. A proof of concept is usually small. In both computer security and encryption, POCs refer to a demonstration that, in principle, shows how a system may be protected or compromised, without the necessity of building a complete working vehicle for that purpose. For example, Winzapper was a POC that possessed the bare minimum of capabilities needed to selectively remove an item from the Windows Security Log, but it was not optimized in any way.[58]

[58] Adapted from Wikipedia

POCs are also used to compare one product to another in terms of functionality or other benefits. It's a try-before-you-buy approach and a low-risk avenue to test the efficacy of a solution that interests you.

Or is it?

POCs are a bit like window shopping at a grocery store: You can look at all the tasty food, but if you don't buy any, you starve to death.

You may feel compelled to launch a POC to help you determine outcomes that are wrapped in product promises but difficult to measure. Before you do, consider these three common pitfalls:

01. **Wasting time evaluating technologies that don't map to your business goals.** There's no point testing what won't produce the outcomes you need, so don't.

    Cautionary Tale: A small community hospital set a goal to invest in cybersecurity starting with fixing all critical and high-priority vulnerabilities so they could reduce business risk and achieve compliance requirements faster. The outcome? They spent three months in POCs testing various vulnerability scanners, but the hospital overlooked the fact that for more than 90 days their vulnerabilities remained unprotected and open to exploitation by bad actors. They would have been better served with an expedited vendor selection process limited to recognizable industry tools and a quick reference check to get to remediation faster, especially since vulnerability scanners differ very little from each other.

02. **Chasing features and functionality rather than pursuing your business goals.** This is the shiny objects trap—avoid it.

    Cautionary Tale: A healthcare provider set a goal to better protect online patient data. Instead, they put security efforts on hold while they waited for upgraded protections promised by a vendor that were never delivered—that were never even built. Like the hospital that lay vulnerable for three months while evaluating new tools, this organization put sensitive PHI at risk as they waited for promised upgrades they never received. The provider believed the vendor's false promise when they should have kept their goals in mind and secured the customer data immediately.

03. **Immobilizing your organization through analysis paralysis.** In your quest for due diligence it's easy to get bogged down by data. If you keep your business goals top of mind, it will be easier to recognize when you've lost perspective.

    Cautionary Tale: Two HCOs came together through a merger. They set a goal to secure all of their collective hardware and software assets—an important early step in an integrated security strategy. The company spent 18 months evaluating new IT asset management products, believing they needed to look outside both organizations' solutions to ensure they were selecting the best possible product, but they became consumed by comparing various benefits among the products and could not make a decision. After nearly two years, they still are running multiple point solutions because they have not been able to complete the integration or achieve any real improvements to ensure all joint assets are properly secured.

The many months spent on POCs won't make your HCO more secure and won't add any value to your bottom line. In fact, you're more likely to wind up hitting the pause button on your entire strategy as you remain trapped in a feature/function bake-off that prevents you from making a decision at all.

And while you're busy getting lost in a maze of interesting features and functions, your HCO lies wide open, vulnerable to cyber attack.

The longer the POC, the longer your business is vulnerable.

LESSON 17

WHAT YOU CAN DO TODAY

If you must enter a POC engagement, do it right. Here are some best practices:

01 Secure executive buy-in first, not after the POC has started.

02 Define success criteria based your business drivers, not on technical features

03 Limit all POCs to 30 days; challengeyour vendor to prove its value in a month, or choose another vendor

04 Identify all gaps between the testing lab and your production environment

05 Understand how the product will be implemented **(see the ICARM approach, below)**

06 Have internal business and technical champions defined for the lifetime the product

07 Establish a process to hold the vendor accountable for delivering and maintaining your defined business outcomes for as long as you own their product

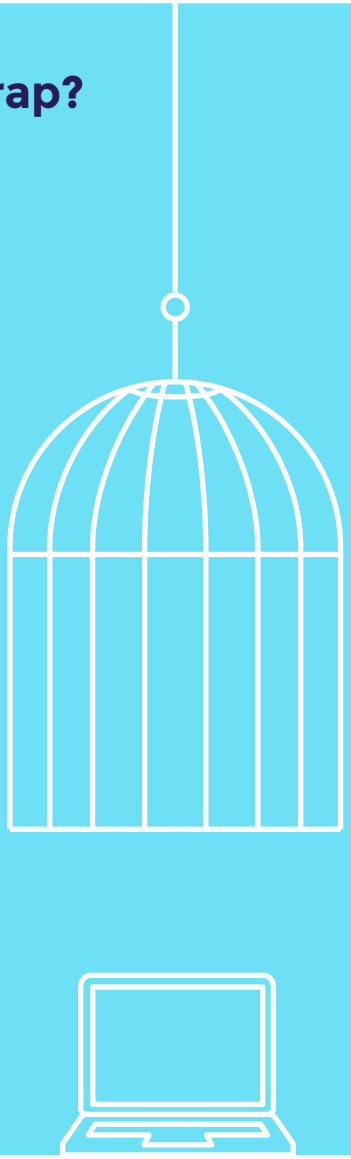
Have You ever Fallen into the Win-Win Trap?

Too often, customers look for what is known as a "technical win;" that is, they look for (and buy) products that meet their technology requirements. But because technology requirements tend to be divorced from business requirements, it's difficult for companies that have not first identified what a "business win" looks like to achieve any real value from their technology investments.

POCs, by their very nature, are designed for the technology win: You can spend months determining whether or not a solution is technologically sound, during which time the business win is sacrificed as your company remains exposed to the very risks you are trying to mitigate.

A further downside to this approach is that it puts even the technical win at risk: The IT team, happy with the results of the POC, faces an uphill battle trying to prove that the technology benefits meet the business need. If the business owners decide they do not, both you and the product company have wasted valuable time.

The features and functions that comprise a technical win will never in themselves add value to your organization. If we've said it once we've said it a thousand times: You have to tie your technology investments to your business drivers if you want to achieve the business win. And you need the right resources and controls in place to keep it.



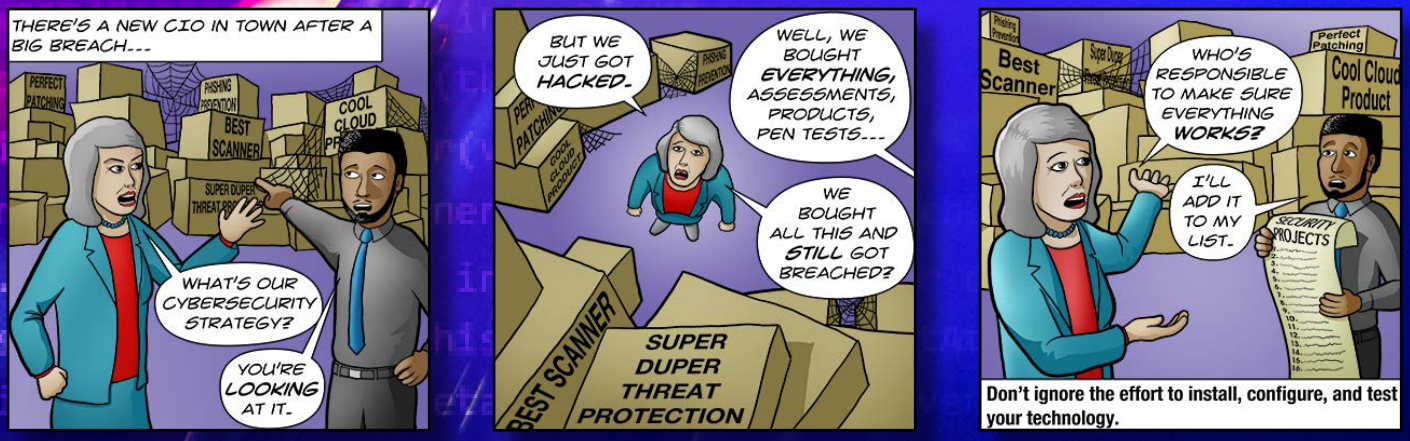
LESSON 18

If you engage a POC, start with the business win; if you don't see a business win within 30 days, consider walking away.

Don't waste time tumbling down the feature/function hole unless you have no other way of evaluating the differences among multiple tools—a side-by-side POC comparison should be the very last arbiter in your decision process.

CHPTR
08

THE WHOLE IS GREATER THAN THE SUM OF ITS PARTS



UNF**KING CYBERSECURITY by CYVATAR.AI

For many decades now, the marriage of people, process, and technology has been a proven best practice, but somehow this union has passed cybersecurity by. The industry has grown comfortable throwing technology over the wall and leaving it up to customers to develop the processes and hire the people necessary to make it work.

It hasn't worked.

The healthcare industry has also failed to adopt the three pillars of people, process, and tech into everyday operations, widening the gulf between cybersecurity needs and overall IT health.

LESSON 19

The best practices for maintaining a secure environment are the same whether you're a small physician practice, a rural community hospital, or a large integrated delivery network. The key for any HCO is to focus on a few high-level priorities, no matter where you are in your security journey.

Make no mistake: Even the largest and most well-funded healthcare organizations have gaps in their security programs and opportunities for improvement. After all, some 80 percent of HCOs have not had a cybersecurity drill with an incident response process, despite the skyrocketing cases of data breaches in the industry. And as we've discussed, outdated IT systems, few cybersecurity protocols, untrained IT staff, and data-rich patient files continue to make HCOs a ripe target for hackers; the willingness of hospitals and physician practices to pay high ransoms to regain their data is a powerful motivator.[59]

PEOPLE: THE FIRST PILLAR

Cybersecurity as a discipline has continued to grow over the past few decades and the IT professionals who have chosen to specialize in it have become some of the most sought after workers in technology. Like any scarce resource—think of the current housing boom of rapidly rising prices and historically low inventory—**demand for skilled cyber practitioners far outpaces the number of qualified professionals to meet it, driving up the cost to hire and retain those resources in-house and making it virtually impossible for rural hospitals, physician groups, and smaller HCOs to compete for them.**

In fact, a 2020 Black Book survey of 291 healthcare industry executives found that cybersecurity roles in health systems take an average of 70 percent longer to fill when compared to other IT jobs. Worse, **75 percent of CISOs said that experienced cybersecurity pros were unlikely to pursue a career in the healthcare industry at all,** primarily because more than any other industry, healthcare CISOs are held responsible for data breaches and the impact on their organization's finances and reputation. At the same time, these CISOs have extremely limited authority over decision-making, technology, or policy.[60]

PROCESS: THE SECOND PILLAR

Security is a process, not a product.[61] In addition to continuous vulnerability assessments and remediation procedures, HCOs need to ensure all technology and security tools are installed and configured correctly and that all issues are remediated as they are found.

Your needs change as your organization changes, and your security solutions should be flexible enough to change with them so that you can continuously remediate new risks and ensure you always receive measurable outcomes from your solutions—that's where ICARM comes in.

[59] Op cit. "Healthcare companies are sitting ducks."

[60] Op cit. "Healthcare Data Breaches."

[61] Schneier, Bruce. "The Process of Security." Schneier on Security. April 2000.

ICARM, or installation, configuration, assessment, remediation, and maintenance, is a methodology for achieving smarter, clearly quantifiable technology solutions.

The current headlines around advanced persistent threats and ransomware attacks, for example, may succeed in keeping you up at night, making the promise of any tool purporting to protect effectively against these threats enticing indeed. Don't be fooled.

ICARM

STEP 01:

Installation & Configuration.

The solution is installed and configured into the HCO's environment.

STEP 02:

Assessment.

Once the technology is up and running, the provider assesses the HCO's environment to identify risks and vulnerabilities.

STEP 03:

Remediation.

Based upon the results of the assessment, the provider will work with the HCO's team to remediate any risks identified rather than just report on alerts HCOs have to track down and solve.

STEP 04:

Maintenance.

The provider stays with the HCO for the duration of the subscription to deliver continuous maintenance, monitoring, and assessments along with monthly executive-level reporting.

LESSON 20

Without ICARM, you'll have a hard time keeping your patient data truly secure.

Few security companies disclose the complexity, difficulty, or sheer effort required to implement and maintain their solutions effectively.

And that makes sense on one level—when was the last time you ran out to buy something you knew would make your life more difficult? But it's also dishonest, and dangerous, because **people's lives and livelihoods may be at stake when security solutions fail to live up to their promise.**

The fact that so many security offerings require a 24/7 SOC or other hefty investments to become fully operational is not information readily offered during the sales cycle. And of course, once the solution is brought in-house and its failings made manifest, it's frequently left to sit on the shelf, without the care and feeding (ICARM) it needs, until it slowly becomes obsolete, never having delivered much (if any) value.

Without ICARM, a clear security strategy, and a process roadmap in place, we remain trapped in an expensive cycle of buying what we think we need or have been told we need and **every shiny new tool that makes its way to market offers more of the same fresh temptation that has failed us every time.**

Much in the way making a purchase out of fear opens the door to new risk, improperly or partially installed solutions also introduce risk to the security environment by creating functionality and integration gaps that are easy for threat actors to exploit.

TECHNOLOGY: THE THIRD PILLAR

HCOs, like organizations everywhere, buy more technology when something goes wrong or when some hot new product hits the shelves. But much in the way your favorite comfort food tastes good, is convenient, and makes you feel better in the moment, it doesn't make you healthy. A technology solution purchased out of fear or familiarity might make you feel good because it's a known entity, but it won't make your practice more secure.

You might spend more money and you might buy more security tools, but you have no way of knowing if you're spending in the right places or on the right things. And you have no tangible way of showing value from your investments. In other words, if you look no further than technology, you may find you've invested in only one-third of a complete solution; without the right people and proven security protocols, the best technology on the market still leaves you vulnerable to attack.

Consider carefully the people, process, and technology you need to extract product value—a company can sell you anything, but without all three security pillars in place, you could become the next Trinity Health.

LESSON 21

Before you buy, take the time to determine the resources required to install, configure, assess, remediate, and maintain the solution you're evaluating so that you can achieve smarter, measurable outcomes that enable you to get to security compliance and cyber-attack protection faster and more efficiently—and show value from your security stack.

Think of the household projects you've attempted yourself and how frequently you received a better end result by calling a professional—well the same is true for cybersecurity. What looks like cost savings at the outset could wind up becoming a whole lot more expensive down the road.

There are almost always unforeseen costs associated with tackling security implementations on your own, up to and including the loss of your job or your company's reputation in the aftermath of a breach.

Can you accurately estimate what it will cost to do the work yourself? Do you have the in-house expertise to implement ICARM methodology? Have you completed successful implementations without help?

WHAT YOU CAN DO TODAY

Here are six questions to ask your security and technology providers to determine if they can support the ICARM approach:

01 Can you install and configure the product for me and ensure it works as promised?

02 Can you train my staff to manage and maintain it, or do you manage and maintain it for us?

03 Can you assess my environment to identify risks and vulnerabilities?

04 Can you remediate the risks you identify rather than just report them?

05 Can you provide continuous monitoring, assessments, and monthly executive-level reporting?

06 How much do your services cost? Are they included with the price of the software?

CONCLUSION: GET CYBERSECURITY CONFIDENCE TODAY

Now that you know the many security challenges HCOs face, what's next?

While there is no silver bullet in cyber, if you approach security investments with your business outcomes as the driver and if you invest in people, processes, and technologies, you will find no limitations on the value you can achieve.

THE MOST IMPORTANT CHECKLIST IN THIS BOOK

01 Start small. Start somewhere. But start.

02 Define what value and outcomes mean to your HCO. If perceived value speaks only to the features or benefits of a product and not to patient safety, data security, or overall profitability, you won't realize value from your investment. Make sure the solution works, that it's aligned to your business outcomes, and that it delivers the results you need.

03 Don't get lost in the compliance maze trying to balance HIPAA, HITECH, and HITRUST; focus instead on advancing your cybersecurity roadmap and compliance will follow.

04 Ensure your MSP, if you have one, is committed to providing true remediation rather than creating more work for you and your team.

05 Use possibility thinking to guide you to alternatives that will enable you to realize extraordinary results and speed time to value regardless of where you are in your security journey.

06 Ensure your security and business goals are aligned at all times.

We're not promising that you'll never get breached if you follow our guidelines, but we do promise that you can achieve dramatic risk reduction and fully realized business value if you train yourself to believe in extraordinary outcomes.

Armed with your checklist and a new way of thinking, you can achieve complete cyber confidence today—confidence that comes from keeping the faith and bringing together the tools, teams, and controls required to keep your security needs and your business outcomes in lockstep. Let us help you get started.

ABOUT CYVATAR

At Cyvatar, **our subscription-based, cybersecurity-as-a-service (CSaaS) membership model takes the worry and guesswork out of security by providing expert practitioners, proven technologies, and a strategic long-term process roadmap at a fixed monthly price** allowing you to succeed at security by:

- **Benefiting from our exceptional talent**
- **Achieving continuous threat remediation**
- **Managing compliance activities**
- **Supporting patient safety and other business outcomes**
- **Proving our value every day**

Not sure of next steps?

Hit us up and let us put you on the road to cyber confidence today.

Cyvatar's CSaaS makes it easy for you to keep sensitive patient data and other confidential information safe, to **feel confident in your security posture and compliance adherence** regardless of whether you're a security practitioner or not.

01 **If you're in the early stages of launching a cyber strategy or lack the internal staff to build one for you, we offer subscription packages that deliver a fully managed security program for any size HCO.** The package includes expert practitioners, proven technologies, and a strategic long-term roadmap for a fixed monthly price. Subscriptions also cover incident response services; IT asset inventory; continuous vulnerability scanning; security gap analysis; and compliance services for standards including SOC 2, CMMC, NIST, ISO, HIPAA, HITRUST, HITECH, and PCI.

02 **If you have solutions in place but struggle with demonstrating the efficacy and value from those solutions, we offer assessments with full and continuous remediation.** Continuous vulnerability scanning and cyber management services ensure that once you achieve remediation you can preserve that solved state over time while maintaining all applicable compliance requirements.

03 **If you're having trouble getting started or don't know what you need, we have a variety of programs, including our virtual CISO (vCISO) package that enables you to execute your security strategy at speed.** Our 100+ years of combined executive and CISO-level experience are at your service, providing top-tier recommendations and guidance and helping you to drive growth while keeping your data and patient information secure.


CYVATAR.AI