# Table of Contents

- **Executive Summary** | 3
- **Introduction: The State of Cybersecurity in Healthcare** | 5

## Emerging Trends
- Interoperability | 7
- IoT | 8
- Virtual Health | 8
- Remote Work | 9
- IT Spending & Training Trends | 9

## Best Practices in Skills Training
- Cloud Security | 10
- Health Information Security | 11
- Risk Management | 11
- Endpoint Security | 11
- Compliance and Controls | 11
- Data Privacy and Security | 11
- Access Management | 11

## Ensuring A Secure Future | 13
The State of Cybersecurity in Healthcare

Executive Summary

The healthcare industry routinely tops the list of U.S. business sectors most financially impacted by data breaches.

Cybersecurity continues to be a growing concern for executives at health systems and health plans alike. Every week, another healthcare organization falls victim to a breach, denial of service, phishing, or ransomware attack that impacts patient health records and personal information. These attacks are becoming more frequent, more dangerous, and more costly: the average breach cost U.S. healthcare organizations an average of $7.13 million per incident in 2020, up 10% from the year prior. This increase is due in part to external threat actors exploiting an industry in crisis as the country reeled from the onset of the COVID-19 pandemic. Those vulnerabilities will not resolve themselves.

Healthcare breaches are especially dangerous, given the fact that they take the most time to identify and contain at 329 days on average. The problem isn’t necessarily a lack of modern security software. More often, it’s a lack of the necessary personnel to achieve an effective security posture. This is just one ripple being felt across an entire industry that has historically lagged in its investments in workforce development.

There’s an assumption that individuals have taken steps on their own to be what the market expects in terms of security. This is largely wrong, because according to the 2017 HIPAA Journal survey, 39% of healthcare organizations say their biggest challenge in cybersecurity implementation is a lack of qualified employees.

Data Breach Stats

$7.13 million
The average breach cost to U.S. healthcare organizations in 2020

329 days
The average days to identify and contain healthcare breaches

39%
say their biggest challenge is lack of qualified employees
It is critical that health systems, health plans, and their partners prioritize the safety of their patients and organizations by investing in the proper people, processes, and technologies.

**People**
Healthcare organizations should begin thinking about cybersecurity as a human resource. This is a problem that stretches across an organization, but should be initiated from the c-suite. Shockingly, only a little over half of all healthcare organizations have a dedicated Chief Information Security Officer (CISO). This lack of cybersecurity leadership can trickle down throughout an organization. According to the 2019 *Verizon Data Breach Investigations Report*, healthcare was the only industry where the majority of cybersecurity incidents stem from inside the organization, with 59% of incidents caused by insiders. Vital health data is 14 times more likely to be compromised incidentally by nurses and doctors than external threat actors. While some of these breaches can be chalked up to human error, most can be traced to improperly trained or untrained employees, privilege abuse, or a failure to implement basic security measures. All require a more strategic solution than ramping up staff awareness.

**Processes**
Recent research shows that many health IT departments are failing to follow some of the most basic steps recommended by the Office for the National Coordinator for Health Information Technology designed to protect patient data. Health systems have only implemented 18% of these recommendations on average, resulting in tens of millions of dollars in HIPAA fines across the industry every year. Proper protocol must be implemented and ingrained culturally across an organization.

**Technologies**
The U.S. healthcare system is grappling with a technology crisis: too many healthcare organizations are operating on antiquated legacy systems while simultaneously integrating new, emerging, and often incompatible technologies, often with little consideration of the resulting security implications. As digital health rapidly evolves, the vulnerabilities created by this gap need to be adequately addressed and managed by a dedicated team of skilled technologists.

Healthcare organizations cannot accelerate cybersecurity staffing fast enough when compared to better-funded, if not also highly regulated counterparts in the financial services industry. The solution lies not necessarily in ramping up hiring and technologies, but in focusing on efficiency by embedding cybersecurity responsibilities within existing IT roles and growing them internally. As healthcare organizations begin to recover from the economic and organizational impacts of COVID-19, cybersecurity threats will continue to evolve and adapt to the vulnerable, shifting landscape. While there are new threats aplenty, the best defense remains the same: maintaining a properly trained workforce.
Introduction

The State of Cybersecurity in Healthcare

The COVID-19 pandemic forced the healthcare industry to confront a multi-pronged challenge when it began spreading across the country in the spring of 2020.

Healthcare providers struggled with lower patient volumes while struggling to care for COVID-19 patients they were ill-equipped to treat, forcing many hospitals to curb revenue-generating procedures.

Health plans grappled with lower utilization while telehealth solutions and remote patient monitoring were adopted quickly. Employees at health plans, health systems, and healthcare service agencies across the country adapted to the same remote work policies implemented in nearly every other industry.

These dynamics placed immense pressure on the healthcare system, the impacts of which were far-reaching across the industry.

These drastic changes put security protocol and infrastructure at risk, creating an incredibly fertile environment for cyber attacks on healthcare organizations and posing a grave threat to the welfare of patients.

Cybersecurity has become a very real patient safety issue, and IT professionals in the healthcare space saw these risks play out frequently in 2020.

Consider the clinical engineer charged with device maintenance in an at-capacity hospital – their ability to repair or securely update equipment as quickly and efficiently as possible is critical to the safety of the patients being treated on-site.
The State of Cybersecurity in Healthcare

These rapid, drastic shifts in healthcare have not been met with equal investment and focus on security. While most health IT budgets increase an average of 9% annually to energize efforts in cloud computing, artificial intelligence, machine learning and other digital transformations, 90% of hospital administrators say their IT security budgets have remained the same since 2016.

Healthcare is sensitive by nature. When it comes to protecting customers, the stakes are higher for organizations operating in the healthcare industry than they are for businesses operating in any other major sector. Even for healthcare organizations whose customers are not patients, it is almost certain that patients are impacted downstream. Now more than ever, there’s a fundamental need to make cybersecurity training a priority to protect healthcare organizations—and, more importantly, their patients.

2020 Cybersecurity Highlights

Healthcare Hackers Begin Jeopardizing Lives

Cyber attacks on healthcare organizations are not only becoming more prolific, but more deadly. One attack on Düsseldorf University Hospital in Germany interfered with a patient’s treatment and ultimately cost a life.

Coronavirus Phishing Scams

Malicious actors preyed on healthcare workers’ COVID-19-related fears throughout the year, luring anxious end users into opening emails exploiting questions and concerns around workplace testing and vaccinations. The success of these campaigns rides on their ability to insert themselves almost seamlessly into the user’s workflow.

Ransomware Attack at Blackbaud

The prolonged attack targeted an outdated component within the cloud service. The breach impacted dozens of providers on Blackbaud’s platform, and hackers managed to compromise the personal data of millions of patients.

New Telehealth Vulnerabilities

The immediate need for expanded telehealth in early 2020 led HHS and OCR to lift penalties against providers using video vendors that are not fully HIPAA compliant during COVID-19. Hackers exploited the loose regulatory environment by targeting popular vendor domains, tricking users into following meeting links, and unknowingly downloading malicious files.
Emerging Trends
Healthcare organizations will need to continue ramping up skeletal network security teams, improving existing cybersecurity protocols, bolstering EHR systems, and fostering a healthy cybersecurity culture in the workplace, while exploring fresh avenues for bolstering privacy and security within both new and long-foreseen technology as compliance trends, outlined below, come to a head.

**Interoperability**

The Office of the Coordinator for Health IT (ONC’s) Cures Act Final Rule, released in March 2020, created exceptions to the 21st Century Cures Act’s information blocking provision and allows patients unprecedented access to their health information through the use of APIs. Health records will have the same access for individuals as bank accounts and investment portfolios, meaning healthcare must meet the same security measures as the financial services industry.

With the rule’s enactment on the horizon in 2021 and 2022, interoperability may be the catalyst for making cybersecurity a true priority in healthcare. This hyper-connectivity between systems, devices, and users will lead to long-sought-after efficiencies and improvements in care and operations—but it will also lead to system-wide security vulnerabilities if each endpoint isn’t effectively managed and monitored in a systematic and competent way.

**IoT**

Health systems across the country are working with myriad connected devices, each with their own set of hardware, firmware, software, backward compatibility, and connectivity characteristics. The average U.S. hospital manages over 19,300 of these devices simultaneously. These assets (or endpoints) can very easily become difficult to track and manage, especially considering their limited level of visibility. The proprietary nature of these devices means most health systems are unable to see which clinical or medical devices are connected to their networks, where these devices are located, and how they’re being operated.

This makes management a nightmare. Without real-time, in-depth visibility, technology management staff will remain pressured to rapidly determine whether or not the latest threat is related to any given device on their network. Device managers are already tasked with retrieving the data produced by devices on an ever-shortening timeline. This combination can prove to be deadly for a healthcare organization and the patients who rely on their devices.
The State of Cybersecurity in Healthcare

The rise of virtual health in 2020 has been meteoric, fueled primarily by dire need during the pandemic. Providers, unable to see their patients in person and eager to make up for drastically decreased volumes, adopted telehealth solutions quickly. Government agencies responded by temporarily relaxing restrictions and easing compliance regulations for communications apps such as Apple FaceTime, Zoom, Skype, Facebook Messenger, and Google Hangouts to allow for a faster transition to virtual health during a national crisis.

This rapid shift to telemedicine and the scale of deregulation it required created a bevy of new issues and risks to information security and privacy. As virtual health became commonplace in 2020, the industry saw a subsequent increase in targeted attacks on telehealth vendors. These attacks threatened patient data across application security, endpoint security, IP reputation and patching cadence, and will continue to do so in 2021. Healthcare organizations will need to partner with cybersecurity experts who can train their staff to safely deploy these resources.

Virtual Health

The rise of virtual health in 2020 has been meteoric, fueled primarily by dire need during the pandemic. Providers, unable to see their patients in person and eager to make up for drastically decreased volumes, adopted telehealth solutions quickly. Government agencies responded by temporarily relaxing restrictions and easing compliance regulations for communications apps such as Apple FaceTime, Zoom, Skype, Facebook Messenger, and Google Hangouts to allow for a faster transition to virtual health during a national crisis.

This rapid shift to telemedicine and the scale of deregulation it required created a bevy of new issues and risks to information security and privacy. As virtual health became commonplace in 2020, the industry saw a subsequent increase in targeted attacks on telehealth vendors. These attacks threatened patient data across application security, endpoint security, IP reputation and patching cadence, and will continue to do so in 2021. Healthcare organizations will need to partner with cybersecurity experts who can train their staff to safely deploy these resources.

Remote Work

As remote work became commonplace across industries in 2020, so did the frequency of social engineering attacks designed to prey on anxieties and curiosities surrounding the pandemic.

Employees, many working with sensitive patient information, are working outside of their offices using home internet connections and personal devices, making them especially vulnerable to malicious cyberattacks that use feigned legitimacy as a guise. Threat vectors, for example, have used fake COVID-19 impact maps like the popular Johns Hopkins’ Medicine tool to spread malware across organizations.
The pandemic has fueled massive growth in IT spending as healthcare organizations strive to meet demand for increased telehealth services, healthcare analytics solutions, and connected clinical and medical devices—all segments of the market that produce visible revenue and directly impact health outcomes. Security spend, by contrast, is lagging by a large fraction.

This is reflected in the lack of adequate cybersecurity staffing. As of Q3 2019, 84% of providers and 65% of payers did not have full-time dedicated cybersecurity staff. In a more recent survey of cybersecurity executives, 74% cited insufficient staffing as the biggest obstacle to maintaining a fully effective security posture, and only 51% of organizations had a dedicated Chief Information Security Officer (CISO).

The lack of properly trained personnel only serves to exacerbate the increasingly complex task of managing evolving cybersecurity risks.

By the Numbers

Security spending has historically lagged across industries, and healthcare is no exception. As pandemic-driven shifts and digital transformation initiatives come to a head, they will create new rifts in information security. It will be increasingly important for providers, payers, and healthcare services to proactively ramp up cybersecurity spending in the year ahead.

Healthcare organizations should take note of the down-trend in cybersecurity and workforce growth in IT budgets, and look to long-term, organizationally-ingrained solutions that will help bolster a skilled, strong, and secure workplace.

Five primary factors are driving IT budget increases in 2021.

<table>
<thead>
<tr>
<th>Segment</th>
<th>2019</th>
<th>2020</th>
<th>2021</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infrastructure Updates</td>
<td>64%</td>
<td>64%</td>
<td>56%</td>
</tr>
<tr>
<td>New Projects</td>
<td>56%</td>
<td>45%</td>
<td>45%</td>
</tr>
<tr>
<td>Cybersecurity</td>
<td>56%</td>
<td>47%</td>
<td>39%</td>
</tr>
<tr>
<td>Workforce Growth</td>
<td>43%</td>
<td>47%</td>
<td>33%</td>
</tr>
<tr>
<td>Remote Support</td>
<td>0%</td>
<td>0%</td>
<td>36%</td>
</tr>
</tbody>
</table>

Source: Spiceworks Ziff Davis, The 2021 State of IT
The shortage of trained healthcare cybersecurity professionals is forcing a mad dash to acquire services and outsource labor at a pace six times more than cybersecurity products and software solutions. In response to the labor crunch, cybersecurity companies are offering healthcare providers with a growing portfolio of managed services.

Health systems and health plans can get ahead of emerging cybersecurity threats by investing directly in skills training across their organizations. It is critical that healthcare professionals understand fundamental cybersecurity concepts and the implications they have in daily responsibilities to minimize organizational and patients’ exposure to risk.

By investing in skills training, healthcare organizations can get the most out of what they’re already spending on cybersecurity from the people they’ve already hired.
Best Practices in Skills Training
Health IT departments are on the front line, protecting patients and their organization from cyber threats.

Healthcare organizations are grappling with a dual need: high demand for robust skill sets, and a high demand for increased, rapid, and continuous training. Both are necessary to maintain a basic knowledge of emerging threats across an organization and hone the ability of staff to identify vulnerabilities and protect against potential dangers.

Optimizing efficiency in skills training requires an understanding of how each role within your organization interacts with and is exposed to cybersecurity responsibilities. Training should be shaped to each individual role and ingrained in day-to-day responsibilities wherever possible.

- **Dedicated Cybersecurity Team.** This category is often much smaller within healthcare organizations but can and should be expanded and leveraged to ensure system-wide security and defense.

- **Cyber-enabled Staff.** This category is composed of IT personnel and workers who handle sensitive data and systems. This should be the target segment for healthcare organizations looking to optimize cybersecurity training spend.

- **General Employees.** All employees require a baseline knowledge of cybersecurity awareness as it pertains to their roles and responsibilities.
Within these population segments, organizations should prioritize increasing skills in these areas:

**Cloud Security.** As the healthcare industry accelerates cloud adoption and usage, organizations must boost the cloud security skills of their cybersecurity and cyber-enabled teams responsible for cloud deployments, data migrations, network and application security.

**Risk Management.** In the face of a growing number of threats and attacks, healthcare organizations will rely on security teams who are adept at identifying cyber threats, assessing which threats pose the greatest risk, and putting the right solutions in place to mitigate impact to the organization.

**Data Privacy and Security.** Patients are increasingly concerned with the protection of their PHI in a time where the data is more accessible than ever before. Organizations need to be able to support a thriving, interconnected digital ecosystem while serving the data security needs of the patients they serve.

**Access Management.** During this time of rapid transition and ballooning telemedicine, organizations are faced with complex levels of identities and access requirements inside and outside of the organization’s walls. A proactive security strategy that actively engages device management staff and secure IT and IoT infrastructure are needed to protect sensitive data and assets.

**Health Information Security.** As the healthcare industry accelerates cloud adoption and usage, organizations must boost the cloud security skills of their cybersecurity and cyber-enabled teams responsible for cloud deployments, data migrations, network and application security.

**Compliance and Controls.** As compliance requirements increase with new legislation, using cybersecurity awareness to “check the box” is no longer a comprehensive approach. Organizations with a proactive cybersecurity strategy meet compliance requirements and are better suited to adapt into the future.

**Endpoint Security.** The prevalence of Internet connected devices in healthcare, referred to as the “Internet of Medical Things,” means a rapidly growing attack surface. All personnel who use, maintain, and implement these endpoints need to protect them from exploitation.
Training for technical cybersecurity concepts is difficult at best. With geographically dispersed, remote work environments, diverse sets of roles and departments, and ongoing busy schedules applying initiatives aligned to personnel day-to-day responsibilities can seem untenable or even impossible. However, it can be accomplished by taking a well-designed, cultural, and multi-modal approach to training.

Healthcare organizations can make training investments meaningful by setting clear, data-driven, measurable goals that align with their cultural and business objectives. Satisfying compliance regulations and ticking off the “cybersecurity awareness training” box is not enough to protect and grow an organization.

Connecting cybersecurity goals—such as certifications, audits, or building internal, system-wide security standards—to cultural and business initiatives is a tried-and-true way to ensure your organization is taking a systemic and proactive approach to cybersecurity.
Ensuring A Secure Future

This is a pivotal moment in the transformation of healthcare, as an entire system simultaneously reacts to a public health crisis and adopts the changes necessary to overcome it.

For healthcare organizations, these changes will inevitably lead to better care delivery, better organizational optimization, and better patient health outcomes. But the rapid deployment of new technologies, paired with the sheer size and depth of their organizational impact, must be approached with a matched investment and focus on cybersecurity. Shifts, like the one healthcare is currently experiencing, can leave organizations exposed and vulnerable; they’re blood in the water for malicious actors in cybercrime.

Despite these technological and systematic changes, the answer to best practices in cybersecurity remains the same. Taking a proactive approach to training that is culturally ingrained, continuous, and targets existing personnel is the most effective and evergreen solution.

Learn more at [www.health.cybervista.net](http://www.health.cybervista.net)

About CyberVista

CyberVista is a cybersecurity workforce development company. Our mission is to build and strengthen healthcare organizations by providing healthcare, health IT and cybersecurity professionals with the knowledge, skills, and abilities needed to drive growth and defense.

Founded in 2016, CyberVista benefits from the rich 84-year history of Kaplan—one of the world’s premier training providers—as its sister company and ally. In 2018, CyberVista welcomed Transcender into the brand. Transcender brings over 25 years of helping organizations and practitioners build technical job skills across all areas of IT and cybersecurity.

Let’s talk.

We look forward to the potential of working with you and your organization on your next initiative.

For further information please email sales@cybervista.net or call 844-558-4782.