KeyBank

# Finding your way to healthcare cybersecurity: Hacking, a digital epidemic

As the first cases of COVID-19 began to make the news, cybercriminals immediately recognized new vulnerability and grew increasingly aggressive. By early March 2020, a major Czech Republic hospital reported being victimized by a significant cyberattack.[1] Days later, the US Department of Health and Human Services experienced a series of attempted hacks, apparently to impede its efforts to fight the virus.[2] Remote workers, including those in healthcare, now encounter heightened online threats, largely in the form of user identity theft and weaponized emails. In the midst of a pandemic, cybercrime flourishes, threatening the safety of every enterprise, including healthcare systems.

Today, online healthcare information is one of the most susceptible, profitable targets for cybercrime. The primary reason: The rapid proliferation of connectivity and medical data has outpaced the implementation of rigorous cybersecurity around healthcare. By learning more about trends in cybercrime, you can make better informed decisions about the computer security systems suited to safeguarding your organization. Because such systems typically require significant investment, this white paper also investigates payment strategies and options.

## Key takeaways

Few documents in contemporary life are as comprehensive and intimate as medical records and other protected health information (PHI).

There are many safeguards your organization can take now — ranging from simple training to sophisticated software systems — to protect your patients, staff, and brand.

Given the rapid proliferation of connectivity and medical data, failing to address cybersecurity shortfalls in healthcare will have catastrophic results.

## The privacy promise

When Congress introduced the Health Insurance Portability and Accountability Act (HIPAA) in 1996, proponents hailed it as an assurance of stringent security and privacy for patient information. The Department of Health and Human Services (HHS) planned to oversee performance of the hospitals, insurers, and related organizations that served as stewards of millions of personal medical records.

### Breaches begin and continue to rise

However, as growing amounts of medical information were digitized and placed online, hackers and other malefactors began to breach computer systems that held the data. In 2010, HHS counted about 200 major data breaches. Over the course of the next several years, HIPAA-related data hacks continued their upward trend, reaching 510 in 2019.[3] It's interesting to note that HIPAA opted to count only those hacks that involved 500 or more patient records. We can only speculate as to how many smaller attacks went unreported. But why are medical records in such high demand by hackers? And why are they so difficult to secure?

### Criminal allure

Few documents in contemporary life are as comprehensive and intimate as medical records and other PHI. Each may hold significant details of a person's medical history, including physician appointments, lab tests, diagnoses, prognoses, medications, supplements, and prescriptions.

Other data commonly specifies a patient's employment history, insurance, credit cards, bank accounts, social security number, demographics, past addresses, and names of relatives.

### Dark web costs

On the dark web (the digital black market), a single stolen credit card might carry a price tag of just twenty cents. In contrast, one medical record could sell for upwards of $1,000.[4] (Whatever the cost, most such illicit sales are often transacted in Bitcoins.) In any case, a stolen medical record commands one of the highest black-market prices for any ill-gotten data. Even the value of a lifted financial record comes in at a distant second place. Why the high price? The illegal possession of PHI and medical records enables high-dollar, high-damage crimes to be committed with impunity. The criminal acts committed typically include identity theft, fraud, and other felonies.

### Dwell time

In most instances, online theft of medical records may remain undetected for weeks or months. Cybersecurity analysts refer to this period (between a breach's occurrence and eventual discovery) as "dwell time." In 2018, median dwell time for hacks was about 80 days, though longer periods are common.[5] Damages to victims can be profound, long-lasting, and far-reaching.

### Illegal physician impersonation

Some data breaches gain access not only to medical records, but to complete sets of physician credentials. These typically command an even higher price than a medical record, especially because the criminal gains the potential to bill multiple insurance companies for countless services, to write prescriptions, and even to pose as a legitimate, practicing doctor.

**A recent study indicated that more than half of healthcare enterprise threats involve imaging devices.**

A hacked device typically means degradation of patient care and theft of patient data. What makes the devices so vulnerable? As of late March 2020, 83 percent of them ran on outdated, unsupported operating systems.[6] Failing to safeguard PHI brings substantial fines and corrective action plans from HHS.

## Why is healthcare a prime target?

Let's consider the three overriding reasons that healthcare institutions make such attractive targets for cybercriminals.

| | |
|---|---|
| **1. Information magnitude** | Compared to most other industries, healthcare keeps an extraordinary volume of data online 24/7.[7] |
| **2. System obsolescence** | Large numbers of healthcare organizations use outdated operating systems and vulnerable applications. (As of March 2020, more than half of medical data breaches involved imaging devices, most of which ran outmoded software.[8]) |
| **3. Security negligence** | Most importantly of all, many healthcare-related institutions have simply "failed to address easily exploitable holes in their security defenses."[9] |

### What's the delay?

These observations raise the question:
**Why have so many healthcare institutions not given cybersecurity the attention and budget it clearly deserves?**
Many industry analysts believe the incredibly rapid expansion of both healthcare data and Internet dependence simply overshadowed the imperative to adopt robust, scalable security.

### Inadequate security

In fact, a substantial number of healthcare executives today admit they need to do more about cybersecurity, even as they witness the inestimable damages of one healthcare data breach after another. In a recent study by Carbon Black, when asked to assign a letter grade to their organizations' cybersecurity quality, most healthcare chief information security officers gave themselves a "C."[10]

### By the numbers

Does this assessment appear exaggerated? Consider these facts: Fifty-three percent of healthcare organizations have undergone a PHI breach within the past year. On average, such a breach exposes more than 7,000 records and costs $1.8 million.[11]

## Data breaches continue exponential growth

While a data breach may seem like the ultimate violation of a computer system's information security, another darker threat looms on the threat horizon: ransomware.

### Ransomware: pervasive threats

Once ransomware takes hold of a single computer or entire network, users can no longer access their computers or the information stored there. A message appears onscreen demanding a hefty payment to restore system functionality. Failure to pay, the message notes, will result in data destruction.

While ransomware continues to serve as a popular, effective tool for cybercriminals, it's impossible to state with certainty how frequently ransomware is used. The reason: Many ransomware victims simply make the payment and, fearing negative press, never report the incident. We've no way of knowing how many organizations have paid ransoms only to lose their data as well, though security analysts observe this occurs commonly.[12]

It is estimated that paid ransom amounts exceeded $7.5 billion in the United States alone.[13] At least one cybersecurity analyst forecasts that by the year 2021 a new business will be victimized by ransomware every 11 seconds.[14]

## Phishing: recognize and mitigate

Whatever your current cybersecurity status, you and your staff could probably use more education and frequent reminders about cybercrime. The reason? Chances are good that once a breach vector is introduced into your work environment, you or anyone with online access will click on a fateful link, open an infected attachment, or trigger ransomware.

Three of the most commonly used methods for introducing a breach to a network are based in phishing techniques. They include emails, attachments, and links, especially those that incorporate counterfeit or "spoofed" URLs. Analysts note that phishing is a source of more than 80 percent of all reported security hacks.[15]

### Questionable email integrity

Most of us are aware of email hacks. You may have seen a colleague's email address hijacked or spoofed in order to elicit a feeling of trust and familiarity. If there are any doubts, speak with (don't email) the sender to verify the communication's validity. Of course, the process adds extra time to the workday, but it's still not as inconvenient as undergoing a cyberattack. If employees receive an email from an unknown source, they should consider deleting it.

Perhaps a particular email appears safe. Even so, links and attachments in the message may still serve as delivery mechanisms for malware, ransomware, and wholesale theft. Here are some ways to avoid initiating a security catastrophe.

### Beware of attachments

If an email includes an attachment, be certain of the file's source. Contact the sender to double-check his/her identity and purpose of the email. If you open the attached file, do not enable editing or enable macros. Close it and bring it to the attention of your IT department.

**Here's the problem:**

A malevolent Excel or Word file with embedded macros often gets past antivirus screening. Opening and editing the file can trigger a string of malicious code that executes some form of attack.

### URL spoofing

URL spoofing works in a similar way. Suppose a familiar address (such as www.abcz-corp.com) appears in an email from a trusted source. Mousing over the URL may appear to verify the address, but the URL still may be counterfeit. Clicking it could lead to a data breach.

- The URL might connect to a perfect replica of the ABCZ website where people freely enter their user names and passwords – directly into a malefactor's database. (Where did the replica originate? "Phishing kits" available on the black market often include counterfeit websites.)[16]
- Alternatively, merely clicking the URL may set off a malware attack on a local PC or the entire network.

### Avoiding suspect URLs and links

- Is it even possible to avoid a spoofed URL or link? In most cases, yes. If you see a URL (particularly in an email, ad, electronic signature, or social media format), just don't click on it. Why not? In many cases, a URL or hyperlink that looks fine is actually composed of counterfeit characters that cosmetically mimic authentic ones. However, if you already know and trust the site referenced by the URL or link, you can visit its home page by typing the address – manually – in a browser.
- If you have any doubt whatever regarding, URL's legitimacy, use a tool to verify it. For example, Google offers a free online "transparency report" to check URL safety. Several antivirus applications incorporate similar functions.
- In the past, a URL prefix of https:// was a fairly safe assurance of a secure site. That's no longer the case because hackers use fake security certificates to impersonate secure sites.

## Low-cost security boosts

While a comprehensive listing of ways to avoid cyberattack is beyond this paper's scope, understanding the security implications of emails, attachments, and URLs is a great place to start. In addition, consider adding the following steps to your security protocol. Most involve minimal or no cost, but they can make a huge difference in cybersafety and efficiency:

- Educate and re-educate employees and contractors on security policies and common threats such as phishing scams
- Use data encryption
- Limit data access only to those employees and others who need it for a business purpose
- Have procedures in place to deal with security threats and breaches
- Remove extraneous data from online access
- Keep all operating systems and applications updated with security patches
- Use multifactor authentication (such as iris scans and fingerprints) to gain access to any secure online data
- If a computer does not need to be kept online 24/7, disconnect it from the internet when it does not require online functionality
- Consistently back up data to more than one storage medium and store backups in more than two secure locations

Even with these precautions integrated into your organization's routine, you'll still need the defensive capabilities of a robust, scalable cybersecurity system.

## Making the secure investment

Industry analysts and internal healthcare IT staff concur: To safeguard data and business viability, ensure that cybersecurity receives a substantial part of the IT budget. Beyond the primary role of safeguarding your data, there are additional valuable benefits of investing in cybersecurity. An effective security system:

- Enables continuity of operations
- Protects reputation and integrity
- Maintains the value of your services
- Costs less than cumulative damages incurred by a cyberattack

You'll find numerous vendors of cybersecurity systems in today's market, many of whom specialize in customized healthcare applications and also provide training and support.

### The price of strong, scalable security

Acquiring a cybersecurity system represents a sizeable investment, and you have several options for handling the expense, including purchase, subscription, or payment plans. A purchase might seem the most direct approach, though it may diminish capital reserves unnecessarily. Using a subscription program can lower cash outlay and provide convenience. However, a customized payment plan also offers convenience, as well as a full range of additional features, including:

- Payments tailored to your budget and initiatives
- Flexible terms: Monthly, quarterly, annual, or multiyear
- Enhanced cash-flow management
- Technology upgrades and protection from obsolescence
- Contract flexibility and control
- Total solution coverage (bundling), including installation, transportation, training, and support costs
- Simplified processing
- Potential tax advantages

Not surprisingly, many US businesses opt for the benefits of equipment acquisition via payment plans.

## Trust your capital provider

In seeking and qualifying a capital provider, look for an organization with proven financial stability as well as demonstrated expertise in healthcare and IT asset experience. A capital provider should also offer:

- An immediate capital solution plus a scalable, long-term strategy
- Innovative structuring knowledge
- Technical acumen and medical-asset experience
- A consultative approach that aligns with your business goals
- Readily accessible in-house credit, legal, underwriting, documentation, and operations experts

In addition, consider the advantages of a capital provider with a proven track record in working with both healthcare and IT professionals. A seasoned capital provider should also understand new technologies and tailor payment solutions with built-in flexibility. In sum, try to find a capital provider that not only expedites equipment acquisition, but also works strategically to maximize your organization's profitability.

## Summary: Facing the challenge

There's never been a period of more promise or peril in online healthcare information. The healthcare industry has the capacity to store and rapidly access detailed patient data that may help save lives and create better futures. At the same time, cybercriminals have proven themselves ever more determined (especially during a pandemic or other emergency) to sabotage, steal, and hold hostage healthcare IT systems in the US and worldwide.

It's incumbent on industry leadership to increase support for strong, expandable online security. Doing so is more than just smart financial strategy. It also builds trust in a healthcare brand and boosts loyalty, retention, and new business. In contrast, failing to take sufficient action on the security front can result in lost business, lawsuits, fines, diminished reputation, or even the end of an enterprise.

Statistics show that every passing day without sufficient healthcare cybersecurity means more and increasingly persistent attacks, breaches, ransoms, and setbacks. We encourage you to take on the challenge of making your healthcare IT environment safer and more secure than ever before, for now and the future. We look forward to working with you.

To learn more about payment plans for healthcare cybersecurity systems, please contact **your Key Sales representative.**

[1]Prague Morning, "Czech Republic's Second-Biggest Hospital is Hit by Cyberattack"
https://www.praguemorning.cz/czech-republics-second-biggest-hospital-is-hit-by-cyberattack/

[2]Bloomberg, "Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak"
https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response

[3]https://www.hipaajournal.com/healthcare-data-breach-statistics/

[4]Forbes, "Your Electronic Medical Records Could Be Worth $1000 To Hackers"
https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#34447aa350cf

[5]https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/ig-mtrends-2019-p1.pdf

[6]MedImaging International, "Majority of Imaging Devices Are Exposed to Cyber Attacks"
https://www.paloaltonetworks.com/resources/research/unit-42-IoT-threat-report-2020

[7]https://www.businessinsider.com/why-healthcare-data-breach-epidemic-will-intensify-2019-4

[8]MedImaging International, "Majority of Imaging Devices Are Exposed to Cyber Attacks"
https://www.paloaltonetworks.com/resources/research/unit-42-IoT-threat-report-2020

[9]HIPAA Journal, "Why Are Hackers Targeting the Healthcare Industry?" https://www.hipaajournal.com/why-are-hackers-targeting-the-healthcare-industry/

[10]Carbon Black, "Healthcare Cyber Heists in 2019" https://www.carbonblack.com/blog/healthcare-cyber-heists-in-2019/

[11]HIPAA Journal, "53% of Healthcare Organizations Have Experienced a PHI Breach in the Past 12 Months"
https://www.hipaajournal.com/53-of-healthcare-organizations-have-experienced-a-phi-breach-in-the-past-12-months/

[12]https://www.cybersecurity-insiders.com/fbi-says-ransomware-victims-usually-do-not-report/

[13]https://www.sentinelone.com/blog/what-is-the-true-cost-of-a-ransomware-attack-6-factors-to-consider/

[14]Cybercrime Magazine, "Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021"
https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[15]CSO, "Top cybersecurity facts, figures and statistics for 2020" https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

[16]CPO Magazine, "Phishing Attacks: Now More Common Than Malware"
https://www.cpomagazine.com/cyber-security/phishing-attacks-now-more-common-than-malware/