

Healthcare Cyber Security

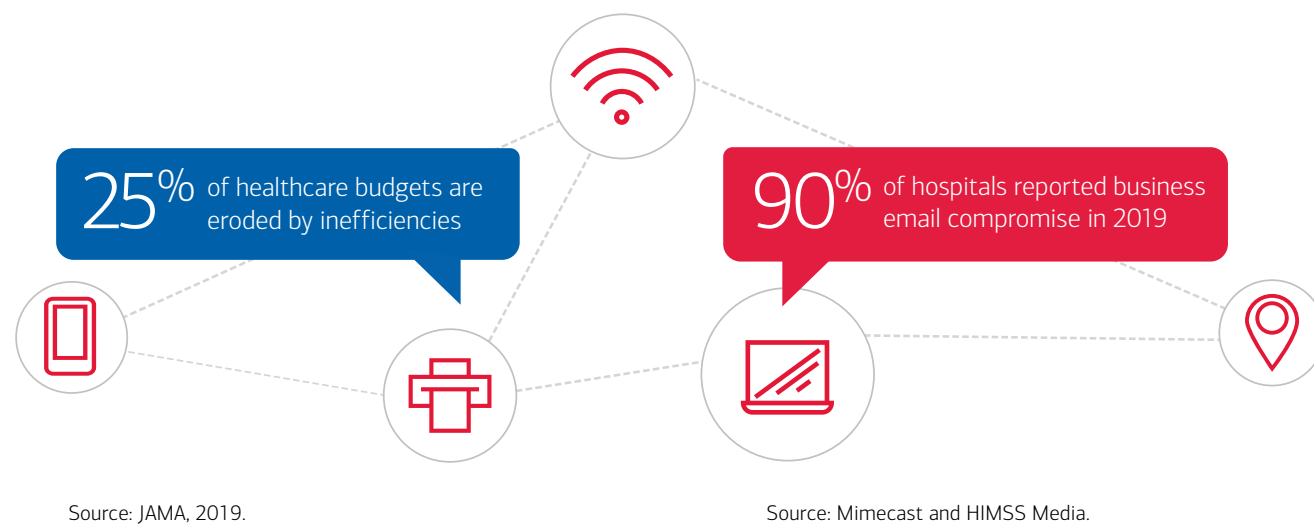
Insights on data safety amid heightened vulnerability



Interconnected technology and patient care

Healthcare organizations rely on vast amounts of data, capturing information on everything from patients' clinical interactions to payer behaviors. This surplus of data has driven the industry to adopt smart devices. The potential benefits to patients and providers are extraordinary. Leading hospitals and health systems have been working to crack the code on consumerism and chronic disease management by delivering a holistic experience for patients, and interconnected technology is essential to these efforts.

Interconnected technology can increase efficiency, but also brings new risks



The benefits of interconnected care delivery are vast. When individual providers are able to quickly access accurate and detailed clinical information, the patient benefits. Better data also supports the kind of sophisticated analysis that allows for improved efficiency and the elimination of wasteful spending and processes. In a 2019 study published in JAMA, researchers conducted a review of more than 50 previous peer-reviewed studies focused on healthcare spending and concluded that waste in healthcare totaled an estimated \$760 billion to \$935 billion between January 2012 and May 2019, accounting for approximately 25% of the total healthcare spend in that period.

Healthcare organizations need data and an interconnected ecosystem of technologies to address some of the industry's most urgent challenges related to patient care and finance. However, becoming warehouses of private health data while expanding the use of more smart devices means hospitals and health systems are particularly vulnerable to cyber criminals. Approximately 90% of healthcare organizations were targeted by business email compromise (BEC) cyber events in 2019, according to research from Mimecast and HIMSS Media.¹ While some cyber criminal organizations pledged to cease targeting hospitals in the early months of the coronavirus pandemic, cyber crime in the healthcare space is alive and well in 2020. As of July 6, *Becker's Hospital Review* had tallied 66 incidents of healthcare providers experiencing cyber events in the first half of 2020.

"Healthcare organizations are a key target for cyber criminals because of the valuable data they hold, and the stakes are high because breaches can become patient safety issues. Awareness and security strategies are essential," said John Hesselmann, Bank of America National Head of Healthcare.

"Healthcare organizations are a key target for cyber criminals because of the valuable data they hold, and the stakes are high because breaches can become patient safety issues. Awareness and security strategies are essential."

John Hesselmann

National Head of Healthcare Banking
Bank of America

The coronavirus pandemic has put a tremendous strain on front-line clinicians and put many cash-strapped hospitals on the precipice of financial insolvency. As hospital leaders work to guide their organizations through unprecedented times, they can't lose vigilance in protecting the data and privacy of their clients, as well as data essential to supporting better outcomes and a better future for healthcare. This e-book provides an overview of healthcare's cyber vulnerabilities and offers insights into how hospital leaders can best protect their organization's data and navigate increased remote access.

The rise of ransomware

Industry best practices

Ransomware is malicious software designed to block user access to computers, data and networks, requiring ransom to be paid in order to release the block or stop the release of confidential or private data. Cyber criminals deliver ransomware in a variety of ways — phishing emails, fake websites configured to look official and pop-up warnings with malicious links to technical support. These methods have become more common across industries, rising sharply year over year. In 2019, more than 200,000 organizations across industries reported successful ransomware campaigns, which marked a 41% increase in these types of incidents from the year before.²

Healthcare is emerging as a primary ransomware target



Source: Emsisoft.

Why are these types of cyber events becoming more common? The answer is simple: ransomware works. In the last quarter of 2019, the average ransomware payment surged to more than \$84,000, which is more than double the average payment for the quarter before. In the last month of 2019, that figure surged once again to more than \$190,000.³

Ransomware is so effective that it has become a profitable commodity for cyber criminals. Organized cyber crime organizations package the software, or create services to manage and execute ransomware campaigns, selling both on the dark web to individuals with rudimentary technical knowledge. To make matters worse, the profitability of ransomware has driven technical innovation. In recent years, major cyber crime groups have honed their social engineering and spear phishing skills, gaining access to an organization's most sensitive information.

For hospitals, health systems and health plans, that information is patient and financial data. When these organizations are compromised by ransomware, the results can be damaging, with incidents of patient data exposure in the hundreds of thousands. Due to the sensitive nature of this information, healthcare organizations can face pressure to pay ransoms. Not complying with the demands of cyber criminals may result in care disruption. This is perhaps why the industry has become such a popular target for ransomware groups. In 2019, healthcare organizations were the most common target for these types of cyber threats with at least 764 providers affected by ransomware cyber crime.⁴

Best practices hospital leaders can leverage to protect their organizations from ransomware campaigns:

- 1. Execute regular backups and testing:** Some ransomware can encrypt local backups as well as primary files. Healthcare leaders should ensure the organization follows strong backup procedures for systems and data. Regularly and automatically back up all of your important business data and information, and store the copies offsite, in multiple locations if possible. However, each organization will have its own cyber risk appetite. Backup and testing plans should be calibrated to each organization's specific needs.
- 2. Update system, security and application software:** Regular technology updates and or patches can minimize many common ransomware vectors. Up-to-date security software makes an organization a more challenging target for cyber crime.
- 3. Assess third-party vendors:** A hospital is only as secure as its vendor partners. Leaders should routinize assessments of vendor access to the organization's network to determine if this access presents unnecessary risk. Leaders must also ensure vendors meet contractual requirements to ensure your networks, systems and data are protected.

Business email compromise

4 preventative steps

The most prevalent vector for ransomware is the inboxes of unsuspecting employees. Emails harboring malicious software are designed to exploit the psychology of employees. The most sophisticated versions of these emails leave staff unaware a breach occurred—instead of concern, targeted individuals may feel as if they had effectively performed their duties by engaging with the email. These emails can be designed to look like internal business communications, prompting staff to share vulnerable information that can be used to compromise an organization's broader technology infrastructure. These types of emails can be especially effective amid moments of extreme disruption, such as the coronavirus, as times of crisis often warrant pivots and changes that can lead to employee uncertainty about appropriate safety protocols. For example, emails to accounts payable requesting invoice or payment changes can pose significant threats in times of uncertainty.

The most prevalent vector for ransomware is the inboxes of unsuspecting employees. Emails harboring malicious software are designed to exploit the psychology of employees.

Four steps hospital and health system leadership can take to protect themselves and staff from falling prey to malicious emails:

- 1. Educate staff on social engineering vulnerabilities:** Provide employees with regular training exercises, such as phishing email or social engineering simulations. Common examples of how cyber criminals leverage social engineering tactics in emails include posing as an approved vendor, posing as an executive requesting payment information from staff, and pretending to be an employee requesting a change in direct deposit information.

Phishing alert: Beware of false email identities



Approved vendor



Senior executive



Seasoned employee

- 2. Regularly update protocols and controls:** The payment approval process for all transactions should be regularly assessed for vulnerabilities
- 3. Limit online exposure for employees with purchasing authority:** Train every employee to recognize that cyber security begins with them and to follow company procedures if they suspect a cyber security incident has occurred.
- 4. Deliver added security training to executives and their assistants:** C-suite executives and their assistants are likely to be the targets of social engineering incidents via email because of their direct access to a host of sensitive information. These staff should be continually trained on the latest cyber security vulnerabilities and encouraged to be vigilant against these threats whenever they peruse their inboxes.

The IoT ecosystem

5 questions to ask

For businesses across industries, the adoption of interconnected technologies has become an inevitability. The Internet of Things (IoT) is transforming business operations in industries such as retail, manufacturing and agriculture. IoT devices are also prevalent in healthcare and becoming more ubiquitous as providers increasingly leverage remote monitoring and telehealth to improve population health and increase safety amid COVID-19. The stakes of keeping IoT devices safe in healthcare, however, are higher than in many other industries due to the sensitive nature of patient health information and the role of technology in delivering safe and effective clinical care.

The IoT ecosystem in healthcare is highly reliant on third-party vendors. For this reason, it is incredibly important for hospital and health system leaders to rigorously vet and continuously assess potential risks from IoT devices and ongoing technology vendor partnerships, including evaluating and implementing the proper segmentation of their network.

While asking these questions prior to integrating new technology solutions can help limit cyber vulnerabilities, the process of keeping IoT devices safe must be an enduring commitment that requires regular assessment. Hospital and health system technology leaders must ensure their teams are committed to raising awareness around the vulnerabilities of IoT devices among staff across the enterprise. Technology teams should be able to identify, locate and assess the potential security risks of every device connected across their organization's network.

Five questions hospital and health system leaders should ask before purchasing an IoT device.

1. Can the solution's firmware or operating system be updated?

The more complex the solution, the more important it is that its firmware or OS be able to update to better protect itself from continuously evolving cyber threats.

2. Will the vendor provide and execute regular security updates?

Before IoT devices are integrated into the system, leaders should know whether these devices will perform regular security updates automatically or if they will need to be prompted to do so by administrators and end-users.

3. What level of authentication can the device support?

Depending on the sensitivity of the information the device is connected to, leaders may want to give special consideration to the device's inherent authentication protocols. For some devices, single-sign-on solutions and two-factor authentications may suffice, while others may merit the implementation of more sophisticated authentication protocols.

4. What level of encryption is available?

Some devices may require added protection, such as layers of intricate code that encrypts data, making it more difficult for malicious software to gain access to sensitive information.

5. Can the device be monitored and controlled from a distance?

Being able to monitor IoT device security performance remotely will allow teams to continuously evaluate and improve the safety of IoT devices.

The mobile threat landscape

6 common vulnerabilities

Mobile technology is an essential component of doing business in the digital age. In healthcare, this technology includes devices and applications used directly for patient care as well as devices used for communicative and operational purposes. While essential, mobile and remote devices present additional challenges for security teams to identify and address. Always connected devices create a continuous stream of digital alerts and emails across a number of devices. This digital overload can cause employees to let their guard down when working outside of the physical workplace.

“Mobile devices and remote working create more access points to a healthcare organization's IT system, making it vulnerable,” said Hesselmann. “Using all your security tools and educating staff can help mitigate threats.”

To better protect staff and patients from potential infection, healthcare organizations around the nation transitioned many administrative employees to remote work amid the coronavirus. While a crucial safety measure, this expanded the scope of networks and devices that have access to healthcare organizations' technology systems.

“Mobile devices and remote working create more access points to a healthcare organization's IT system, making it vulnerable. Using all your security tools and educating staff can help mitigate threats.”

John Hesselmann

National Head of Healthcare Banking
Bank of America

Six common forms of cyber crime all staff should be aware of:

1. **Phishing and smishing:** Email and text messaging scams can be especially effective on mobile device screens that may cut off key message details.
2. **Vishing:** Cyber criminals will call either from supposedly trusted sources or robocalls with urgent messages to scam staff into turning over money or protected information.
3. **Malware:** Spyware, banking malware, ransomware and adware can be designed to target vulnerabilities in both personal and company-issued mobile devices and apps.
4. **Hacking of applications on devices:** Cyber criminals can take advantage of encryption vulnerabilities on mobile apps to bypass user login credentials and gain access to the system or device.
5. **Network spoofing:** Cyber criminals may set up fake Wi-Fi hubs to pry passwords and personal details from remote workers and travelers.
6. **Password compromise:** Data can be lost or compromised if an employee's password is insecure, overly simplistic or compromised after being obtained through phishing.





Supporting a cyber secure home

4 steps to share

All remote hospital staff should be educated on how to maintain a safe security posture from a work-from-home environment. Here are four steps leaders can share with staff to support a cyber secure home office.

- 1. **Follow all company data privacy policies:** If staff must print hard copies of files, they should not be viewed by family or roommates and should be securely disposed of after use.
- 2. **Protect the router and physical workplace:** Screens should not be visible by others, and default router passwords should be changed.
- 3. **Work-issued devices should be used by employees only:** Staff should be instructed not to allow anyone else to use their work devices and to power down all devices when not in use.
- 4. **Utilize all layers of the organization's security policies:** All security tools and software updates should be fully integrated into all staff mobile devices.

Focus on the fundamentals




This is a vulnerable moment for America's health systems. The coronavirus pandemic has placed a significant strain on front-line staff and revenue streams, and the transition to more remote work may heighten a healthcare organization's risk of experiencing a cyber event. Authorities can gather evidence after a cyber event — which can potentially result in recouped funds down the road — but preventing an event from happening is the responsibility of hospital leadership and staff. Outfitting on-site systems with a strong cyber security policy is crucial. However, amid the disruption of the coronavirus, leaders should pay special attention to mobile and remote security measures. Perhaps nothing is more important than ensuring staff are familiar with the basics of cyber hygiene: Think before clicking, use strong passwords and regularly back up data onto company servers.

True preparedness includes being ready to act swiftly and effectively in the event of a cyber event.

Even with the integration of leading protection technologies and regular staff training on the fundamentals of cyber security, there is no guaranteed, 100% effective ransomware prevention strategy for healthcare organizations. True preparedness includes being ready to act swiftly and effectively in the event of a cyber event. If a health system does experience a ransomware incident, technology teams and staff should remove infected devices from the network as quickly as possible to potentially localize the malicious software. Transparency with patients and staff about cyber events is also essential to supporting recovery, as not disclosing such matters can tarnish a hospital's reputation and compromise patient loyalty.

“By staying up to date on cyber security trends, educating staff and preparing for attacks, healthcare organizations can protect patient data and help stop fraud before it occurs,” said Hesselmann.

Cyber hygiene staff basics

-  Think before clicking
-  Use strong passwords
-  Conduct regular data backups

¹[mimecast.com/resources/press-releases/dates/2020/3/himss-research/](https://www.mimecast.com/resources/press-releases/dates/2020/3/himss-research/)
²[nytimes.com/2020/02/09/technology/ransomware-attacks.html](https://www.nytimes.com/2020/02/09/technology/ransomware-attacks.html)
³[nytimes.com/2020/02/09/technology/ransomware-attacks.html](https://www.nytimes.com/2020/02/09/technology/ransomware-attacks.html)
⁴blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/#:~:text=In%202019%2C%20the%20U.S.%20was,in%20excess%20of%20%247.5%20billion



By your side.
So you can be
by theirs.

Caring for people is what you do. Caring for businesses like yours is how we've served the healthcare industry for decades. Bank of America Healthcare Banking™

BANK OF AMERICA 

"Bank of America" and "BofA Securities" are the marketing names used by the Global Banking and Global Markets divisions of Bank of America Corporation. Lending, other commercial banking activities, and trading in certain financial instruments are performed globally by banking affiliates of Bank of America Corporation, including Bank of America, N.A., Member FDIC. Trading in securities and financial instruments, and strategic advisory, and other investment banking activities, are performed globally by investment banking affiliates of Bank of America Corporation ("Investment Banking Affiliates"), including, in the United States, BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp., both of which are registered broker-dealers and Members of SIPC, and, in other jurisdictions, by locally registered entities. BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp. are registered as futures commission merchants with the CFTC and are members of the NFA.

Investment products offered by Investment Banking Affiliates: Are Not FDIC Insured • May Lose Value • Are Not Bank Guaranteed.

©2020 Bank of America Corporation. All rights reserved. 3339738 09-20-0547