Healthcare Is Fighting a Deadly and Costly Threat:

Cyber Attacks

5 Strategies to Protect Your Healthcare Organization

DIGITAL SOLUTIONS • PROFESSIONAL SERVICES • INFORMATION TECHNOLOGY

RICOH
imagine. change.

A September 2021 Ponemon study reported the following:[1]

- Over the last two years, 43% of respondents said their HDOs (Health Delivery Organization) experienced a ransomware attack. Of those, 45% said they believed the attack resulted in a disruption of patient care operations.

When asked about that impact:

- 71% reported a longer length of stay for patients,
- 70% cited delays in procedures and tests,
- 65% said there was an increase in patient transfers or facility diversions,
- 36% pointed to an increase in complications from medical procedures, and
- 22% said mortality rates increased.

The combination of the COVID-19 pandemic and a ransomware epidemic has had devastating, and sometimes deadly, results for even the best prepared hospitals and health systems.

Why Healthcare Is Such a Target

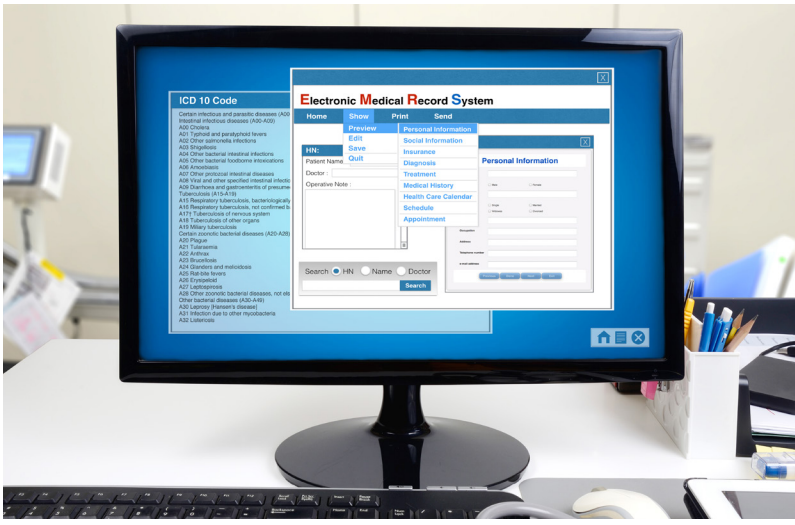
The cyber threat to patients and to healthcare systems is an attack on two fronts. The first is the risk to patient care and the potential loss of life that can result due to an attack. The second is the financial, data, and security risk. Both make HDOs more attractive targets for hackers.

More and more HDOs are having to pay significant ransom payments to reopen virus-impacted systems. A recent report from Sophos stated, "More than a third of healthcare organizations were hit by a ransomware attack in 2020 and of those, 65% said the cybercriminals were successful in encrypting their data."[2]

Ransomware isn't the only threat. Hackers are also after medical data and personal, nonmedical information included with healthcare records. This data is extremely valuable on the black market because it can be used for identity theft and financial fraud.

The Wall Street Journal reported, "Among nearly 1,500 data breaches at health-care entities in the U.S. from 2009 to 2019, affecting 169 million patients…The disclosure of nonmedical information that could be exploited for identity theft or financial fraud—such as driver's license numbers, Social Security numbers and bank account or credit-card numbers—was much more common."[3]

The distributive nature of healthcare and the need for closer collaboration of multiple, separate entities to provide continuity of care also increases the vulnerability for HDOs. Another challenge for small to midsized health systems and rural hospitals is the lack of cybersecurity skills and the required investment.



5 Strategies to Protect Your Healthcare Organization

All of this can feel overwhelming for healthcare leaders responsible for protecting their organizations, but there is hope. Just like vaccines are used to fight the spread of viruses in humans, cybersecurity can help slow or even stop the spread of viruses and malware across the healthcare IT landscape.

As the old saying goes, "Necessity is the mother of invention." As cyber attacks grow in frequency, cybersecurity is keeping pace. A recent article in *Cybercrime* stated, "Cybersecurity Ventures predicts the global healthcare cybersecurity market will grow by 15 percent year-over-year over the next five years and reach $125 billion cumulatively over a five-year period from 2020 to 2025."[4]

Ricoh is proud to be part of the solution. Our team understands the difficulty of balancing security and risk with efficiencies and outcomes. Utilizing Ricoh's IT Management & Cloud Services for healthcare can help you protect patient information and comply with changing regulatory mandates. In addition, Ricoh's Security and Governance products like RansomCare can also help limit your organization's vulnerability and risk to ransomware.

Consider these five strategies to help build awareness and compliance to lessen the severity of a hack—not if, but more likely when it happens.

1) UNDERSTAND AND MONITOR DATA ACCESS POINTS

More than half of attacks were carried out by an insider. Keep in mind this could be an employee, business associate, or other third party with access to the system.[5] At the same time, take a close look at vendors and clearinghouses that receive and send patient data to be sure information is secure on both ends. Check to confirm vendors' patient data management processes meet HIPAA guidelines and that vendors have their own cyber security program in place.

Other recommendations:

- Monitor access to workstation technology and output devices such as multifunction devices, traditional printers, and fax machines to avoid breaches.
- Consider shifting to digital fax technology to avoid the proliferation of information-sensitive paper copies.
- Identify areas of risk and employ technology and services that enable healthcare organizations to remain hyper vigilant in identifying areas of weakness and vulnerability.
- Review control safeguards that help identify lapses in data and device security. Also, shared devices that are critical to patient care may require a unique set of security safeguards.

2) LOCK DOWN WORKSTATIONS AND MULTIFUNCTION DEVICES TO HELP PREVENT UNAUTHORIZED ACCESS

Healthcare's connectivity across technology devices and systems gives hackers more places to enter the system. Some technology has built-in safeguards such as badge scanning, thumbprint recognition, or other user authentication mechanisms that can help detect breaches. However, it can help to confirm that security tools are installed and fully implemented in each device.

3) CONDUCT COMPREHENSIVE ANNUAL RISK ASSESSMENT AT LEAST ONCE A YEAR

Identify and understand the threats to the organization based on recent cyber attacks in healthcare and other industries and by using input from technology vendors. Include actual hacking attempts based on real-life scenarios of data management systems and processes to evaluate vulnerability. Consider hiring professional hackers as security watchdogs to test the network and the cloud and to identify gaps in the system. At the same time, use mock hacks and phishing email attacks to not only test employees, but to also identify where additional staff training may be required.

It can help to include mobile devices in the assessment to verify proper use in conjunction with both cyber security and HIPAA requirements. Combine all assessment findings to create and test a cyber attack response plan, which can include well-defined downtime procedures for processing information handwritten on paper until the system is back up and running securely.

Cyber security professionals from Ricoh can help you develop a comprehensive cyber attack response plan. Our goal is to make sure that your organization is prepared in advance of an incident.

4) EDUCATE EVERY END USER ON CYBER SECURITY IN ADDITION TO HIPAA REQUIREMENTS

Only 25% of IT professionals across all industry segments are confident in employee cyber security awareness.[6] In fact, the same group indicated the first improvement they would make to bolster cyber security is increased employee training. This starts by helping staff and physicians differentiate between cyber security and HIPAA requirements.

To be successful, training should be administered repeatedly and cover both pre-emptive behaviors and post-incident reactions. As mentioned earlier, sending out mock phishing emails is a great way to train and test employees. Consider training staff on the appropriate procedures to follow when they suddenly

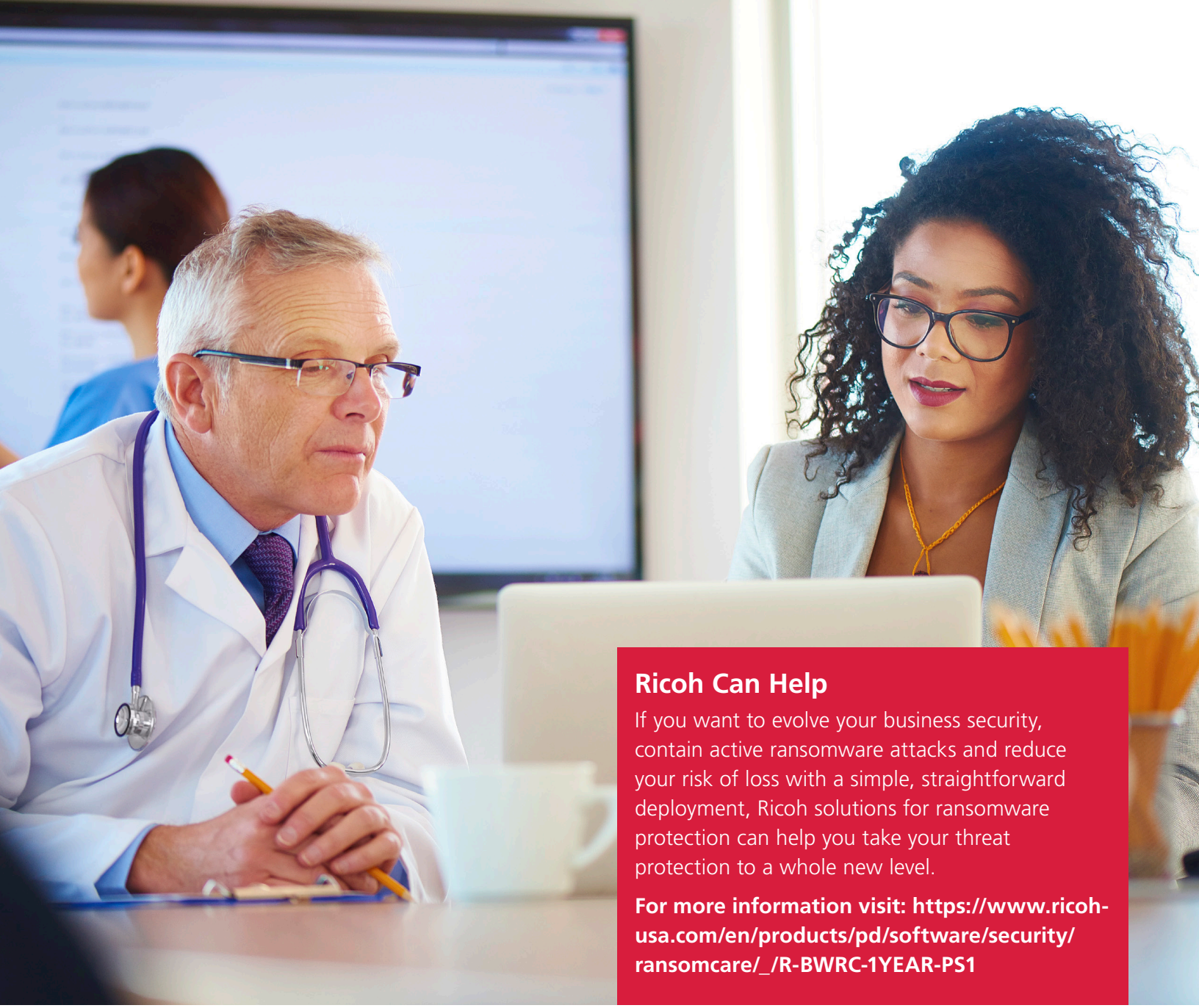
can't access files on a shared server or experience some other unusual event while on the system. Include actual examples of seemingly harmless hacker techniques such as phishing emails with malicious attachments or URLs that can infect and even disable the entire system with one click.

5) REVIEW HOW BUSINESS SYSTEMS AND PROCESSES SUPPORT SECURITY

A thorough analysis of all aspects of data collection, storage and use can help drive improvements and support tighter cyber security measures. Include these key business systems as part of an internal review of cyber security preparedness:

- **Business Process Optimization** — Examine current processes and operations to help identify security gaps while also looking for ways to improve efficiency.
- **Asset Management** — Monitor vulnerabilities by constantly scanning and reporting enterprise technology assets regardless of make, model, or location and how those assets work together to help support the organization.
- **Content Management** — Evaluate how clinical and administrative data is captured and linked to internal systems to help improve business and clinical processes in a way that can reduce exposure.
- **Fax Server** — Confirm the secure organization and flow of internal and external information between internal and external devices.
- **Forms Management** — Review the capture, management, and flow of clinical and administrative information to help guarantee that data is safely and securely handled, as well as to help reduce the chance of information mismanagement and human error.
- **Interoperability** — Look at all the different ways that patient data is typically shared, from an unstructured, analog method to a digital, electronic transfer method.

- **Output Management** — Monitor and audit enterprise printing to help address the need for confidentiality, misdirected or forgotten print jobs, or unauthorized access.
- **Point of Service Scanning** — Assess how capturing and directly linking clinical and administrative data to internal systems at the point of service can help reduce potential exposure.
- **Hardware** — Gauge how well the organization uses hardware by examining steps such as user authentication at the printer, encryption to help safeguard documents, data, address books, passwords and more, automatically overwriting latent digital images and managing unstructured data.



Ricoh Can Help

If you want to evolve your business security, contain active ransomware attacks and reduce your risk of loss with a simple, straightforward deployment, Ricoh solutions for ransomware protection can help you take your threat protection to a whole new level.

For more information visit: https://www.ricoh-usa.com/en/products/pd/software/security/ransomcare/_/R-BWRC-1YEAR-PS1

1 https://www.healthcareitnews.com/news/ponemon-study-finds-link-between-ransomware-increased-mortality-rate

2 https://www.healthcaredive.com/news/more-than-13-of-health-organizations-hit-by-ransomware-last-year-report-f/602329/

3 https://www.wsj.com/articles/how-to-prevent-medical-records-from-being-hacked-11592605721?mod=ig_cybersecurityreport

4 https://cybersecurityventures.com/healthcare-industry-to-spend-125-billion-on-cybersecurity-from-2020-to-2025/

5 http://www.fiercehealthit.com/story/healthcare-no-1-target-cyberattacks-2015/2016-04-20

6 http://business-reporter.co.uk/2016/03/21/only-quarter-it-professionals-confident-employee-cyber-security-awareness/