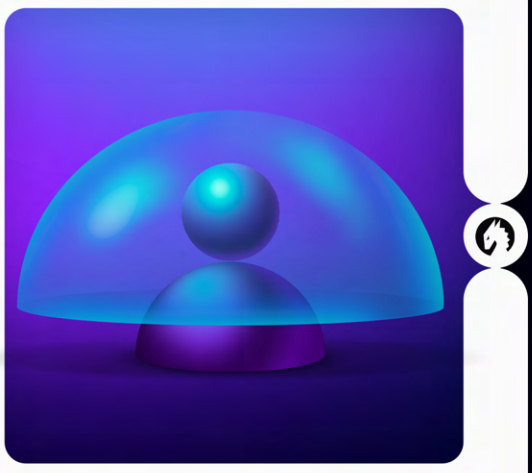
ironwall
by Incogni

Healthcare providers and ransomware prevention



Executive Summary

As healthcare providers grapple with the rapidly growing and costly risk of phishing and ransomware attacks, and the danger they represent to personnel, patient safety, and professional reputation, as well as the cost of legal and financial liabilities, forward-thinking providers are exploring preventative and reactive measures to address these challenges.

Personal information is the gateway that enables many forms of personal, cyber, and financial attacks. Since 2011, Ironwall has delivered online privacy protection that finds and removes personal information (home address, cell phone number) from the Internet, as well as security services that prevent personal content from appearing online before it can be shared or sold. Our service protects employees, service providers and patients potentially affected by a breach, along with additional protection against future hacks.

Healthcare vs. Ransomware

Horror stories about ransomware targeted at healthcare providers have been impossible to avoid because they just keep coming. According to an analysis by the cybersecurity firm Emsisoft, 46 hospital systems suffered ransomware attacks in 2023, up from 25 in 2022 and 27 in 2021. Across those 46 attacks, at least 141 hospitals were directly affected and experienced disruption due to a lack of access to IT systems and patient data. And these are just the incidents that have been disclosed.

Every week, it seems another prominent target is invaded by computer code that locks out personnel from the essential services they provide. “Almost every hospital CEO I speak to now [says] that cyber risk is their number one or number two enterprise risk issue,” says John Riggi, national adviser for cyber security and risk at the American Hospital Association (AHA), which represents hospitals and healthcare networks. “It’s one of the main issues that keep them up at night.”

The breadth and seriousness of the problem can be illustrated by a closer look at some of the specific attacks that have occurred or been announced recently:

May 2023

A data breach at North Carolina's Columbus Regional Healthcare System compromised the patient names and Social Security numbers of 132,000 people.

August 2023

Singing River Health System in Mississippi suffered a ransomware attack that resulted in a data breach impacting 252,890 individuals. The stolen files contained names, addresses, phone numbers, Social Security numbers, credit or debit card information, tax identification numbers, passport numbers, usernames and passwords, prescription information, medical record numbers, and health insurance information.

December 2023

The Wichita Urology Group said more than 5,000 people may have been affected by a breach — the second in a year to hit the medical practice. At about the same time, the Kansas Joint and Spine Specialists in Wichita reported a "cybersecurity incident" that impacted nearly 400 patients and employees.

November 2023

The emergency rooms at New Jersey's Pascack Valley Medical Center and Mountainside Medical Center were forced to shut down, and no new patients were admitted after a ransomware attack on their internal systems.

January 2024

An attack on technology company HealthEC exposed almost 4.5 million records belonging to patients signed up to 18 U.S. healthcare providers. For Michigan's Corewell Health, it was the second time in a matter of months the organization's patients found themselves victims of a major data breach due to an attack targeting one of its suppliers. Approximately one million patients were impacted by that attack.

January 2024

Ardent Health Services filed a notice of data breach with the Attorney General of Texas after discovering that it was targeted in a ransomware attack. In this notice, Ardent explained that the incident resulted in an unauthorized party being able to access consumers' names, addresses, phone numbers, email addresses, Social Security numbers, medical treatment information, health insurance and claims information, and Medicaid or Medicare numbers.

In addition to hospitals and healthcare systems, hackers are now also targeting patients directly. Providers such as Seattle-based Fred Hutchinson Cancer Center and Oklahoma City-based Integris Health have reported that their patients have received emails attempting to blackmail them; a tactic hackers hope will apply additional pressure on providers to pay the ransom. Attacks on plastic surgery centers have resulted in intimate images being publicly posted. One group demanded $50 per patient to delete their data.

There is currently no greater security challenge to healthcare IT systems than ransomware. However, while these and countless other occurrences suggest that healthcare providers are losing the war, it is also true that the overwhelming majority of attempted breaches are successfully thwarted.

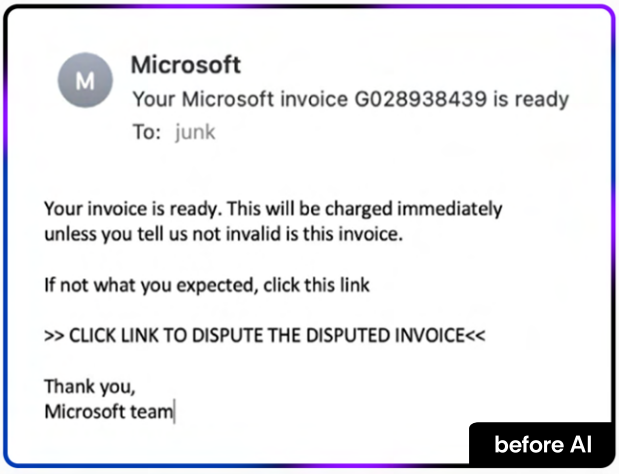
The US Department of Health and Human Services has instituted standards for hospital cyber security and levies significant fines for non-compliance. But while billions of instances of malicious traffic are blocked every year, many still succeed. As one network security expert commented, "We're outgunned."

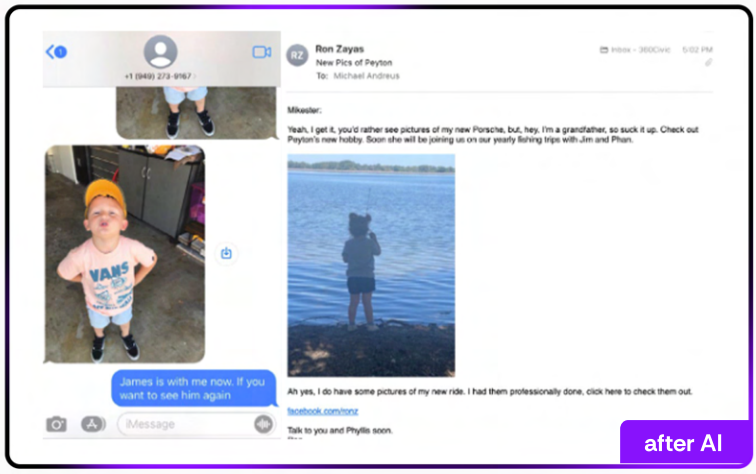
Why Are So Many Ransomware Attacks Successful?

Ransomware is computer code, or malware, that is deployed into a network with the intent of disabling systems. Deployment methods vary, but exploited vulnerabilities (38%) and compromised credentials (30%) are among the most common root causes of the most significant attacks. More and more, however, email-based attacks (malicious emails or phishing) have become the starting point for a successful breach.

"Our Employees Wouldn't Fall For That"
Don't be too sure. Hackers have come a long way from the obvious scams they tried ten years ago. Today's thieves are combining the adaptability of artificial intelligence with the copious amounts of personal data available freely on the Internet to tailor individual emails that are amazingly effective.

Instead of a one-size-fits-all email, hackers now harvest the emails of the organizations they want to attack, identify key individuals, and automatically write scam emails that incorporate the recipient's name, address, family members, hobbies, mobile number, and even photos and videos in a way not possible even two years ago.





If someone receives an email that includes names of relatives, or photos and videos of family members, it's easier to believe it may be authentic. If that employee clicks on the link in the email, his device is compromised, and the network is compromised. That typically results in exposed credit card numbers and social security numbers, exposed patient information, lawsuits, insurance claims, unfavorable news stories, and more headaches than providers can imagine.

After a system has been crippled, the attacker will make contact and offer a key that will unlock any blocked data – for a price. Payment is requested in cryptocurrency such as Bitcoin, as this makes the transfer of funds harder to trace.

Higher Stakes, Higher Payments

An attack on a retailer can stop customers from buying items online, and perhaps obtain data on credit cards used to make purchases. But when a hospital's systems are compromised, lives are put at risk.

Without access to patient records and essential IT systems, hospitals must put their emergency departments on redirect, and send ambulances to other nearby healthcare facilities. When every second counts, the consequences can be fatal.

In addition, locked-down systems mean canceling and rescheduling appointments, long delays in receiving test results that are necessary for accurate diagnosis and treatment, and longer hospital stays for patients.

One study, conducted by McGlave, Neprash, and Nikpay of the University of Minnesota School of Public Health, found that in hospital mortality for patients already admitted at the time of a ransomware attack increased. The attacks also caused a 17%- 25% reduction in hospital volume during the initial attack week, and they estimated that between 2016 and 2021, ransomware attacks killed between 42 and 67 Medicare patients.

Given these outcomes, the pressure on healthcare agencies to restore service is greater, which is also why hackers realize they can demand higher payments. According to the Verizon Cost of a Data Breach Report, the average cost of a healthcare data breach increased to its highest-ever level in 2023, costing an average of $11 million, a 53% increase since 2020.

How Can Healthcare Providers Protect Themselves?

As one public official commented after an attack, "Paper and pencil seem to work pretty well against those kinds of things." However, as that solution is no longer practical, some action plan is essential. The objective should be to reduce the likelihood of becoming a target, and to limit the damage to employees and patients should a breach occur, which can greatly reduce a provider's legal and financial exposure.

A logical place to start is by identifying the vulnerabilities that make ransomware attacks possible. The first line of defense should not require a large investment in technology or personnel – all it takes is vigilance on the part of anyone with access to the provider's online network.

Since most phishing emails are now ransomware, a cybersecurity awareness and education program is one of the most effective steps a company can take. Make sure all personnel (physicians, support staff, executives) understand how to spot phishing, and how to maintain the habit of smart password management. And if someone slips and does click on something hazardous, stress the importance of reporting it immediately, which can help to limit the damage.

The next key to combating a ransomware attack is to make sure all of the stored data is backed up. Such backups are only effective if they are continuous (some cloud services run 15-minute interval backups) and if the data is saved on a system that is either not always online or requires authentication. Test those backups regularly.

Many providers have adopted the 3-2-1 rule, which means three backups, in two forms of media, with one of them offsite. The offsite backup must be in a system that is not connected to the main network. If the backups are in a different building but still on the same network, they are also at risk.

With the 3-2-1 rule, in the event of a ransomware attack, a provider can be back in business in a matter of hours, by wiping its servers and refreshing from the backup.

While email is the most common method of entry for ransomware, this malicious code can also enter a system when a hacker scans the Internet for systems with open ports that are exposing Remote Desktop Protocol (RDP), virtual network computing (VNC), or other remote administration services, and hijacking those services to get access to victim servers.

Scanning tools such as Nmap, masscan, and Shodan can detect any exposure. Some systems have also added port switches as an extra precaution. When a port detects abnormal traffic, the switch shuts it down at the port level and alerts IT personnel, so they can determine if there is a problem.

In addition, a new type of cyber security software — "extended detection and response" or "XDR" — can gather data from IT applications, networks, hardware, and email traffic, and sometimes uses artificial intelligence to monitor threats in real-time.

Additional steps that can be taken include:

- Review all firewalls for vulnerabilities
  Install anti-virus software (it won't always work but it can help)
- Periodic penetration and vulnerability assessments
- Disabling macro scripts from office files transmitted over email
- Cybersecurity insurance (it won't prevent attacks, but it can mitigate the financial burden of recovery if the worst happens)

Who Is In Charge?

It is imperative to know who will be responsible for guarding against ransomware attacks. There is often confusion over this, especially when smaller budgets have resulted in smaller staff. If the internal IT department consists of one person, it's asking a lot for that person to implement every ransomware precaution while still fulfilling his or her other daily obligations in places with multiple servers and hundreds of terminals.

For this reason, many providers are turning to outside security firms with the experience and resources to combat the ransomware threat. These companies will assess a provider's security status, and take appropriate steps to implement additional precautions as part of a multilayered security program. They will also schedule regular assessments and audits of the network's security posture, to make sure best practices are being maintained.

Since AI and tailored attacks need information to prosper, privacy protection providers can also lower the level of information available to a provider's personnel, which makes them more elusive targets. When the personal information of a provider's employees is removed from data brokers, people finder sites, governmental sites — anywhere it can show up on a search engine — it means scammers have less to go on.

Scrubbing every personal information detail from every employee in a firm that employs hundreds, or thousands, may seem like an impossible task. But it is important to understand that hackers pursue the easiest targets, and those where their attacks have the greatest probability of success. If an AI-inspired phishing scam finds just two pieces of information on one hospital's staff and 50 on a competitor's, they will always go after the hospital where they have more content to exploit.

Protection – Even if the Worst Still Happens

A preventative plan protects providers from the inevitable attacks that are launched every day. But if the worst has already happened, they can also constrain the damage. By receiving constant monitoring and feedback, personnel will be alerted as their information is found and removed. These plans can also reduce losses incurred from lawsuits, employee defections, and even patient class action suits. Insurance carriers cover most post-breach services.

Conclusion

The risk of ransomware has grown exponentially in recent years and shows no sign of receding. However, it is possible to significantly reduce the risk of infestation by building secure defenses, educating employees about the guises of ransomware, and leveraging the expertise of companies experienced in data protection.

Get Started: Protect Yourself Now

If you're a healthcare worker concerned about your own safety, or manage a team that you'd like to protect, Ironwall is ready to go to work for you.

Request a Quote for Your Organization