# Cyberattacks: Not a Matter of If, but When

Kerri Reeves

**Kerri Reeves** is a contributing editor based in Ambler, PA.

Cyberattacks have become commonplace in healthcare. In fact, 88% of surveyed healthcare organizations experienced at least one cyberattack in the past year.[1] While 44 million Americans were affected by health information breaches in 2022, the number skyrocketed to 106 million last year, impacting one in three people.[2] In the past four years, the Office of Civil Rights (OCR) has seen a 239% increase in large breaches involving hacking and a 278% increase in ransomware attacks.[3] These occur every 11 seconds, and a data breach, on average, costs $9.23 million.[4]

For cybercriminals involved in identity theft or fraud, personal health information (PHI) is big business. Stolen health records sell up to ten times or more than credit card numbers.[5] Recent targets include Shields Health Care Group, a Massachusetts-based medical imaging service provider that had 2.3 million patient records exposed by a cybercriminal,[6] and California-based Regal Medical Group, a victim of a ransomware attack that compromised the PHI of 3.3 million patients.[7]

"It's a big problem," says Christoph Wald, MD, PhD, MBA, professor and chair of the Department of Radiology at UMass Chan-Lahey in Burlington, Massachusetts. Dr Wald warns that owing to the widespread nature of vulnerabilities, "Sooner or later, you will find yourself in the situation [of an attack]."

Comprehensive cybersecurity—protection of equipment, networks, and systems from digital attacks—is necessary in today's healthcare climate to maintain quality services and safety of patient data. It is particularly important in radiology, where legacy imaging systems remain prevalent. A department's oldest imaging assets may be based on obsolete operating systems and often cannot be equipped with modern cybersecurity protection software.

"From a radiologist's perspective, you're always managing [up to] 20 years of legacy technology in your department," says Dr Wald, adding that without regular security patches, vulnerabilities will persist, putting entire organizations at risk.

## Potentially Severe Consequences of Cyberattacks

For radiology, which is operationally dependent on resources connected through local and wide-area networks, an attack's impact can be extensive. Image output, creation, transport, review, interpretation, dictation, and report distribution are digital and rely largely on integration with health information systems, radiology information systems (RIS), electronic health records (EHR), and picture archiving and communication systems (PACS).

"Radiology is the first digital specialty. We are completely and 100% dependent on these systems and networks," Dr Wald says. "When we get attacked, the whole chain of imaging care may break down immediately—with potentially immediate effects on patient care depending on the clinical setting."

Numerous financial, logistical, and patient care consequences may result when operations are compromised. The University of Vermont Health Network (UVMHN) in Burlington, Vermont, was targeted by a major cyberattack in 2020. Kristen DeStigter, MD, chair of the Department of Radiology and chief of Health Care Service at the system, says that impact was significant.

"This was complete devastation," says Dr DeStigter, who revealed that their entire infrastructure,


including more than 5,000 end-user devices across 1,300 servers, were affected by malware.

She said the attack occurred after an employee opened a seemingly ordinary email attachment on their laptop at a coffee shop. Ten days later, when connecting to the health system's network, a Trojan virus hidden within that attachment infiltrated the network, allowing malicious actors to deploy additional malware to probe other parts of the network. Soon, ransomware reached a virtual server and began encrypting all virtual hard disks, resulting in a widespread system outage. While the network's EHR was not impacted, it was shut down proactively.

While medical imaging technology and associated integrated networks have vastly improved care for patients, the seamless connectivity can make entire health systems vulnerable to security breaches and subsequent complications. Patients may need to be rerouted to neighboring institutions, experiencing compromises or delays in imaging care. Further, in-hospital mortality goes up 20 to 35% for patients admitted during a ransomware attack.[8]

UVMHN experienced 39 days of downtime in outpatient imaging, resulting in "serious financial consequences," says Dr DeStigter, citing losses of more than $63 million. Fortunately, there were no untoward patient outcomes.

Other cyber targets have become defendants in class action lawsuits resulting from the exposure of PHI,[9] which can also result in penalties running into the millions of dollars levied under the Health Insurance Portability and Accountability Act (HIPAA). Banner Health, for example, was penalized $1.25 million for HIPAA violations discovered after a massive data breach.[10]

In November, North Carolina-based US Radiology, which has operations in New York State, agreed to pay a $450,000 fine following a ransomware attack that exposed PHI of nearly 200,000 patients after the company failed to remediate a vulnerability.[11] New York Attorney General Letitia James said that patients "deserve confidence," stating "In the face of increasing cyberattacks and more sophisticated scams to steal private data, I urge all companies to make necessary upgrades and security fixes to their computer hardware and systems."[11]

## Preparedness and Protection

In establishing a cybersecurity strategy, radiology leaders must prioritize protective measures to limit vulnerabilities across their organizations and preparedness for attacks. Indeed, they must be ready to switch to analog mode at a moment's notice.

"My biggest piece of advice is to be prepared. Treat your preparation like a mass casualty drill," Dr DeStigter says. "The downtime workflow should be well established and practiced multiple times."

She says UVMHN kept eight workstations operational with 24/7 radiology coverage. They had no computers, PACS, RIS, connected workstations, dictation, email, pagers, or Internet except for patient Wi-Fi systems.

"Our entire system went into a 'downtime procedure' we had never practiced," says Dr DeStigter, adding that the department had to quickly buy paper, printers, pens, and other supplies.

Most radiology departments simply are not prepared for suspension of digital operations, Dr Wald says.

"When it happens, it's going to be a mess, so it's important to have some building blocks of functioning," he observes, referring to ensuring the availability of and accessibility to paper forms,


filing systems, processes, and modality-specific working groups.

## Steps to Ensure Secure Systems

From a hardware and software standpoint, the American College of Radiology (ACR) recommends that the information technology departments of healthcare facilities, including radiology, be sure to:[4]

- regularly update and patch operating systems on imaging and other equipment;
- encrypt data on physical media and data in transit;
- manage security software, including authentication and passwords;
- tightly control data access on a need-to-know basis;
- establish secure configurations of networks;
- perform regular equipment audits to ensure procedures are followed;
- perform penetration testing and regular vulnerability assessments; and
- consider end-point protection in the form of individual firewalls to protect especially critical equipment.

"Everyone has a piece of the responsibility to defend our devices," Dr Wald says, adding that radiology leaders should stress cybersecurity awareness as the foundation of department-wide policies and behaviors.

While securing technology to reduce vulnerabilities is important, humans—who are constantly creating, interacting with, and sharing data—are the vital link in cybersecurity.

"If you had to pick one thing to do [for cybersecurity], the human side is the most effective bang for the buck," he says, citing a statistic that 90% of cyber incidents are related to human behavior, including clicking on phishing emails, using weak passwords, or failing to update software.

Dr Wald says educating employees about not clicking on unfamiliar links or opening attachments in suspicious emails, only using organization-approved USB drives; not downloading information from untrusted websites; and safeguarding laptops from unauthorized access is vitally important. All employees should be aware of cyberthreats, common entry points, and potential consequences. They should also have a safe and simple way to speak up and report anything out of the ordinary.

Unfortunately, none of these measures is fool proof.

"Protection will not result in the absence of an event however small or big, so being prepared at least to the point that you have some concept of what you're going to do if you go down [is important]," says Dr Wald, advising that one person in the department should be tasked with ensuring cybersecurity and preparedness as part of daily operations.

## Know the Drill

Mapping out an imaging enterprise's information ecosystem so radiology managers understand which functions are performed in-house and which ones are managed by external IT vendors is also beneficial. By establishing how various systems are

connected, radiology leaders can determine how to stay operational when "the lights go out," as well as who to contact about specific concerns, Dr Wald says, which enables continuity of patient care and instills department-wide confidence.

Conducting simulated cyberattack drills is also a good idea; they help employees learn how to recognize potentially threatening emails and respond to suspicious events, as well as to identify areas for improvement. Connecting radiology with other departments enables the entire facility to share information and resolve complications.

Radiology department leaders should also work with their equipment vendors to maintain security of legacy systems. If a vendor-run program isn't available, IT and cybersecurity companies are available to help implement measures such as isolating a resource from the rest of the network with firewalls, Dr Wald explains.

The Cybersecurity and Infrastructure Security Agency, the Department of Health and Human Services, and the Health Sector Coordinating Council Cybersecurity Working Group all offer providers tools, resources, training, and information.[12] In addition, the ACR's IT Commission Cybersecurity Work Group hosts a cybersecurity resource page with helpful how-tos, primers, videos, links to government resources and chat forums, as well as recommendations for recovery strategies.[4]

At UVMHN, site of the most significant healthcare cyberattack of 2020, Dr DeStigter recalls the impact on the organization's finances, employee morale, and patient care.

"It took seven months for us to come back fully in radiology," she says, noting that some 300 employees were furloughed or reassigned because of the attack. She also recalls the disappointment of oncology patients whose prior studies were rendered unavailable to help assess whether their treatments were working.

"We thought we were secure. No hospital is secure," says Dr DeStigter, who urges collaboration and investment in cybersecurity measures to safeguard patient data and maintain the uninterrupted provision of medical imaging services.

"Hospital administrators and their IT department should ensure radiology is prioritized and well-protected," she concludes.

## References and Resources

1) Olsen E. 88% of healthcare organizations experienced a cyberattack in past year, report finds. Healthcare Dive. Published Oct. 11, 2023. Accessed Jan 30, 2024. https://www.healthcaredive.com/news/88-percent-healthcare-organizations-report-cyberattack-ponemon-institute/696358/.

2) Southwick R. Healthcare cyberattacks have affected more than 100 million people in 2023. Chief Healthcare Executive. Published Dec 18, 2023. Accessed Jan 30, 2024. https://www.chiefhealthcareexecutive.com/view/health-data-cyberattacks-have-affected-more-than-100-million-people-in-2023.

3) HHS' Office for Civil Rights Settles Ransomware Cyber-Attack Investigation. U.S. Department of Health and Human Services. Released October 31, 2023. Accessed Jan 30, 2024. https://www.hhs.gov/about/news/2023/10/31/hhs-office-civil-rights-settles-ransomware-cyber-attack-investigation.html.

4) Welcome to the Cybersecurity Resource Hub. American College of Radiology. Accessed via Jan 30, 2024. https://www.acr.org/Practice-Management-Quality-Informatics/Informatics/Cybersecurity-Resources

5) Riggi J. A high-level guide for hospital and health system senior leaders. AHA Center for Health Innovation. Accessed via Jan 30, 2024. https://www.aha.org/center/cybersecurity-and-risk-advisory-services/importance-cybersecurity-protecting-patient-safety.

6) Petkauskas V. US medical provider hack impacts 2.3m+ victims. Cybernews. Published Nov 15, 2023. Accessed Jan 30, 2024. https://cybernews.com/news/shields-health-care-group-data-breach/

7) Diaz N. 11 lawsuits filed against California medical group over ransomware attack that affected 3 million patients. Beckers Hospital Review. Published March 15, 2023. Accessed via Jan 30, 2024. https://www.beckershospitalreview.com/cybersecurity/11-lawsuits-filed-against-california-medical-group-over-ransomware-attack-that-affected-3-million-patients.html.

8) Levi R. Ransomware attacks against hospitals put patients' lives at risk, researchers say. National Public Radio Oct 20, 2023. Accessed Jan 30, 2024. https://www.npr.org/2023/10/20/1207367397/ransomware-attacks-against-hospitals-put-patients-lives-at-risk-researchers-say#:~:text=HANNAH%20NEPRASH%3A%20During%20a%20ransomware,at%20the%20University%20of%20Minnesota.

9) The Top 15 Healthcare Industry Cyber Attacks of the Past Decade. Arctic Wolf. Published Aug 22, 2023. Accessed Jan 30, 2024. https://arcticwolf.com/resources/blog/top-healthcare-industry-cyberattacks/

10) Davis J. Banner Health pays $1.25M penalty over HIPAA failures from 2016 breach. SC Media. Published Feb 2, 2023. Accessed Jan 30, 2024. https://www.scmagazine.com/analysis/banner-health-pays-1-25m-penalty-over-hipaa-failures-from-2016-breach.

11) Greig J. NY AG issues $450k penalty to US Radiology after unpatched bug led to ransomware attack. The Record. Published Nov 8, 2023. Accessed Jan 30, 2024. https://therecord.media/new-york-attorney-general-fines-radiology-firm-after-ransomware-attack.

12) Healthcare and Public Health Cybersecurity. Cybersecurity and Infrastructure Security Agency. Accessed Jan 30, 2024. https://www.cisa.gov/topics/cybersecurity-best-practices/healthcare#:~:text=Together%2C%20CISA%20brings%20technical%20expertise,issues%20in%20HPH%20every%20day.