

## How to Prepare for, Survive, and Recover From a Cybersecurity Attack: A Guide for Radiology Practices—AJR Expert Panel Narrative Review

*Benoit Desjardins, MD, PhD, Marla B. K. Sammer, MD, MHA, Alexander J. Towbin, MD, Patricia Balthazar, MD, MPH, Richard Staynings, MS, Po-Hao Chen, MD, MBA*

<https://doi.org/10.2214/AJR.25.33354>

Accepted: July 21, 2025

Article Type: AJR Expert Panel Narrative Review

Article Section: Multispecialty

*The complete title page, as provided by the authors, is available at the end of this article.*

### Abstract

In an era of persistent and evolving cyberthreats that pose serious risks to patient safety, institutional integrity, and regulatory compliance, healthcare organizations, particularly radiology departments, must adopt a proactive stance toward cybersecurity. Radiology departments are particularly vulnerable to cyberattacks due to their dependence on often legacy and insecure digital imaging systems, as well as a reliance on network connectivity and specialized software. This AJR Expert Panel Narrative Review offers a strategic roadmap for healthcare institutions to prepare for and survive cybersecurity attacks, with a focus on the unique vulnerabilities within medical imaging systems that radiology departments must address. Real-world threats, ranging from PACS network exploitation to DICOM data manipulation, ransomware disruptions, and the consequences of inaction are examined. Emphasis is placed on practical defense mechanisms including layered security architecture, regular vulnerability assessments, employee training, and incident response simulations. The insights are intended to inform a defense-in-depth strategy incorporating physical, technical, and administrative safeguards aligned with HIPAA and other regulatory standards. Overall, this guide for radiology practices seeks to align technical controls with operational resilience, to aid practices in detecting, containing, and recovering from cyber-incidents with minimal disruption to patient care.

### Recommended citation:

Desjardins B, Sammer MBK, Towbin AJ, Balthazar P, Staynings R, Chen PH. How to Prepare for, Survive, and Recover From a Cybersecurity Attack: A Guide for Radiology Practices—AJR Expert Panel Narrative Review. *AJR* 2025 Jul 30 [published online]. Accepted manuscript. doi:10.2214/AJR.25.33354

The publication of this Accepted Manuscript is provided to give early visibility to the contents of the article, which will undergo additional copyediting, typesetting, and review before it is published in its final form. During the production process, errors may be discovered that could affect the content of the Accepted Manuscript. All legal disclaimers that apply to the journal pertain. The reader is cautioned to consult the definitive version of record before relying on the contents of this document.

## Introduction

In today's digitally driven healthcare environment, cybersecurity is not just a protective measure but a vital foundation for building trust between patients, practitioners, and healthcare organizations [1]. As digital technologies like EHR, PACS, medical imaging devices, and Internet of Things (IoT)-enabled medical devices become increasingly integrated, the importance of protecting sensitive patient data and clinical research has never been greater. However, as healthcare technologies evolve, so too do the risks [2].

Cybersecurity in healthcare is built upon three fundamental pillars of confidentiality, integrity, and availability [3]. Confidentiality ensures protection of sensitive patient data. Integrity focuses on preventing unauthorized alterations to medical records. Availability requires efforts to keep healthcare IT systems, along with the growing network of medical devices, operational.

Sensitive data, including medical records and images, are prime targets for cybercriminals. A breach not only threatens patient privacy but also undermines the trustworthiness of healthcare organizations, disrupts essential services, causes financial losses, and, in extreme cases, endangers patient lives [4].

Healthcare privacy and security regulations like the U.S. HIPAA, Canadian Personal Information Protection and Electronic Documents Act, European General Data Protection Regulation, Australian Privacy Act, and various Personal Data Protection Acts of Singapore and many neighboring countries, add a regulatory requirement to protect personal health information for all regulated entities that directly or indirectly provide medical services.

Given these high stakes, healthcare organizations must prioritize cybersecurity preparedness. This *AJR* Expert Panel Narrative Review explores strategies that healthcare institutions can adopt to prepare for, withstand, and recover from cybersecurity attacks while ensuring the protection of sensitive data and continuity of patient care. In addressing the topic, we highlight the unique vulnerabilities within medical imaging systems that radiology departments must address.

## Cyberthreat Landscape in Healthcare

Many ways exist to illegally and illegitimately read, copy, change, delete, or temporarily make unavailable critical healthcare data and the systems needed to access such data, thereby disrupting modern digital healthcare services. Some of these attack vectors have been used in actual cyberattacks, whereas others have been identified as theoretic or potential risks by researchers. This section describes the most common cyberthreats against healthcare and ways in which radiology departments may be affected (Table 1).

### *Common Cyberthreats in Healthcare*

**Data breaches**—Data breaches pose significant and ongoing threats to healthcare organizations given the vast amounts of sensitive personal and medical data they manage. The 2009 HIPAA security regulations mandated reporting any data breach involving more than 500 medical records [5]. Since then, nearly 7000 such breaches have been reported in the United States, the largest being the Change Healthcare breach in 2024 involving 190 million medical records [7] (Table 2). Ongoing attacks ensure the presence of a constant stream of breaches under investigation. According to the Department of Health and Human Services Office for Civil Rights, cumulative U.S. healthcare breaches have resulted in the loss, theft, exposure, or impermissible disclosure of 846,962,011 healthcare records as of May 2025 [6]. Among a U.S. population of 340 million, very few individuals have avoided some breach of their personal identity information or personal health information (PHI). Although approximately two-thirds of breaches are caused by hacking, often from external attacks, some breaches result from insider threats and unauthorized data access [6].

Healthcare data breaches typically do not cause immediate physical harm to patients, but they can severely damage patient trust and lead to regulatory noncompliance. Thus, regulators require corrective action plans to address noncompliance, in addition to fines and punitive damages. Indeed, financial repercussions can be enormous, reaching hundreds of millions of dollars in fines, restitution, and costly class action lawsuits. For example, the Change Healthcare breach is expected to incur costs of up to \$5 billion [7]. The costs of other cyberattacks that impact availability, like ransomware, can be even greater.

**Phishing and social engineering**—Phishing attacks often serve as the initial entry point for more substantial breaches. These attacks typically involve cybercriminals tricking individuals into revealing sensitive information, including passwords, through fraudulent emails or phone calls [8].

A common phishing technique involves deceptive web links that entice recipients to click. This method was used in the Anthem breach in 2015 (the second-largest reported medical records breach to date) [9] (Table 2). Another frequent tactic is to attach a malicious file to an email. If opened, the attachment can install malware on the user's computer and lead to a breach, as occurred in the University of Washington Medical Center breach in 2013 [10] (Table 2). Spear phishing involves a targeted attack against a particular individual, perhaps a systems or security administrator, or a financial controller, chief executive officer (CEO), or other senior executive.

Social engineering refers to behavioral manipulation techniques used by cybercriminals to trick individuals into divulging confidential information or performing actions that compromise security. These tactics frequently accompany phishing attacks, manipulating staff into inadvertently granting access or installing malware. Healthcare employees, who are often busy and under pressure, are particularly vulnerable to such deception.

According to KnowBe4 and Trend Micro, more than 90% of cyberattacks start with a phishing attempt [11] while 32% of all successful breaches involve phishing techniques [12]. Continuous employee security education, training, and awareness (SETA) can mitigate the risks of phishing and social engineering [13]. A strong inverse correlation exists between current SETA programs and click rate by staff [14]. Indeed, security leaders widely acknowledge the huge return on investments of ongoing and multimodal security training programs, especially in healthcare environments.

**Ransomware attacks**—Ransomware has emerged as one of the most damaging threats to the healthcare sector [15] (Table 2). The combination of large volumes of PHI and the industry's low tolerance for downtime makes healthcare a prime target for ransomware attacks and other forms of cyberextortion [16]. At least 60% of healthcare institutions have been victims of attempted or successful ransomware attacks [15].

In typical ransomware attacks, malicious actors gain access to a system and then encrypt critical medical data, making them inaccessible. They then demand a ransom for the decryption key. These attacks can cripple hospital operations for weeks [17], delay treatments, and lead to patient safety concerns with associated morbidity, and, in some cases, mortality [4] (Table 2). Ransom attacks have even led to hospital closures [18]. The potential impact on patient care and practices' long-term financial viability from disruptions in system availability is a key factor driving ransomware and other forms of cyberextortion in healthcare. [19]

Because of the urgency to restore healthcare systems after a ransomware attack, organizations may choose to pay the ransom even when data backups are available [20]. Attackers often increase the pressure to pay the ransom by stealing medical data before encryption and then threaten to release it, a tactic known as secondary or tertiary extortion [21]. However, paying the ransom does not guarantee data recovery or protection from future attacks. A total of 92% of organizations do not get all of their data back even when extortion payments are made quickly [22], and the time needed to restore and validate recovered data can take months, often negating any value derived from a ransom payment when one is made. Indeed, ransom payments, especially by healthcare practices, is a primary driver for the growth of this illicit industry.

Robust cybersecurity measures are essential and should include comprehensive backup and recovery protocols, resilient high-availability system architectures, and well-practiced incident response and business continuity plans.

Security programs should include robust holistic policies, standards, procedures, and guidelines combined with technical and physical controls. The most successful security programs are ones where a uniform culture of cybersecurity is present and actively sponsored by the board and CEO. Controls, however, must balance usability with security and privacy to optimize enterprise organizational objectives. As an example, hospital security leaders have implemented stronger multifactor authentication (MFA) for

radiologists while concurrently implementing greater single sign-on. The increased time and effort of an MFA logon is thus equalized by greater convenience and removal of the need for staff to log in to each application or system separately—a mutual benefit for imaging staff and hospital security.

## Specific Threats to Radiology

*Disruption of radiology workflow*—Radiology departments, while not typically the direct target of cyberattacks, are highly vulnerable due to their reliance on technology and network connectivity [23]. When radiology systems such as PACS are compromised, the event can delay diagnoses or treatment timelines, disrupt radiology workflow, and even lead to missed diagnoses if critical images are unavailable [24].

*Attacks on radiology hardware and software*—In radiology, diagnostic imaging examinations, including radiography, MRI, and CT, are vital for patient care. These images are stored and shared through PACS, making these systems highly vulnerable to cyberattacks. A successful attack can result in theft, alteration, or destruction of critical diagnostic images, risking patient safety [24].

In the late 2010s, three different cybersecurity groups scanned the Internet, searching for unprotected medical imaging devices. They discovered over 36,000 unprotected devices [25], including image servers exposed to the Internet. They then informed each exposed entity of their discovery and advised them on how to protect their devices. Six months later, one of the three groups repeated the search to assess compliance. Surprisingly, the follow-up scan found even more unprotected imaging servers [26], illustrating the ongoing vulnerability of medical image storage systems and the weakness of medical imaging security programs.

Beyond hardware exposure, radiology is also at risk from vulnerabilities in the software used to view, process, and report diagnostic images. These applications provide a wide attack surface for cybercriminals. For example, in February 2025, the Philips DICOM medical image viewer software was compromised by an Advanced Persistent Threat (APT) [27]. The exploited vulnerability allowed attackers to install a backdoor, enabling unauthorized access to the institution's network.

*Data corruption and manipulation of diagnostic images*—Data corruption or manipulation of diagnostic images poses a significant risk in radiology. This issue is illustrated by two proof-of-concept studies. In 2020, a cybersecurity team in Israel entered a hospital during the night and connected a small device to intercept CT images being transmitted from a CT scanner to the PACS [28]. Deep-learning software was then used to alter the images, either inserting or removing lung nodules. The tampered images were convincingly altered, fooling up to 99% of radiologists, highlighting the danger of undetected image manipulation. In a separate study, researchers in Spain showed how malware could be

embedded within a DICOM file, potentially allowing attackers to take full control of a radiology department's systems [29].

The risks posed by corrupted or manipulated diagnostic images extend beyond patient care. Healthcare organizations are legally and ethically bound to ensure the accuracy and integrity of medical records, and any alteration of diagnostic images undermines trust in the healthcare system, potentially leading to severe legal consequences.

## Preparing for a Cyberattack in Radiology

Because each step of the radiology workflow depends on technology, preparing for cyberattacks requires a comprehensive approach that addresses infrastructure, workflow, risk, and personnel [30] (Table 3).

### *Risk Assessment, Threat Modeling, and Layered Security*

In radiology, risk assessment begins by identifying vulnerable digital assets, such as PACS, modality workstations, diagnostic workstations, and data repositories, and then evaluating the likelihood and potential impact of various cyberthreats on each. The HIPAA Security Rule outlines three categories of safeguards: physical, technical, and administrative [31]. In radiology, these categories translate to securing physical access to imaging equipment, implementing robust network segmentation, and enforcing stringent protocols that outline who can approve and perform system changes, respectively [32].

Threat modeling involves the envisioning of how attackers might exploit vulnerabilities to gain unauthorized access, disrupt workflow, or compromise data integrity. Common approaches such as STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) guide security teams to think systematically about potential modes of attack [33]. For instance, an attacker may first scan for publicly exposed DICOM endpoints such as a misconfigured PACS. Unauthorized access may enable image tampering using generative algorithms [27]. Alternatively, a denial-of-service attack may be attempted from a trusted network device to other radiology devices and modalities [24]. Buffer overflow attacks may also occur with DICOM endpoints [24]. Enumeration of these threats in advance may allow development of high-value mitigation plans, including restricting user privileges, enabling intrusion detection systems, and deploying strong encryption at rest and in transit.

Risk assessment and threat modeling then inform design of a layered security or defense-in-depth strategy [34]. The intent is to ensure that, if one defensive measure fails (e.g., an employee inadvertently clicks a phishing link), another layer (e.g., limited user privileges) might still block or contain the breach. In practice, radiology departments can accomplish this aim by deploying multiple overlapping safeguards across physical, technical, and administrative domains aligned with HIPAA Security Rule regulations [31]. At the physical

layer, server rooms and control consoles are kept behind locked doors, and critical hardware is accessible only to authorized personnel. At the technical layer, solutions might include firewalls, network segmentation, antivirus and antimalware software on imaging workstations, continuous user and systems monitoring for anomalies, and strict role-based access controls that limit each user's permissions to the minimum necessary for their role. Other measures, including the adoption of zero trust principles across healthcare, are beginning to address and reduce the industry's inherent vulnerabilities [35]. Administrative layer controls complement these measures through policies that govern software changes, login session timeouts, enterprise change management, and other control mechanics.

## Cyberhygiene

**Regular updates and patching**—Maintaining up-to-date software is a cornerstone of cybersecurity. Attackers often exploit known vulnerabilities in operating systems, third-party components, and specialized imaging software that radiology departments use daily. Prompt patching and version updates narrow these windows of opportunity, reducing the likelihood of successful exploits.

However, radiology faces unique challenges with patch management. Imaging equipment often operates continuously, leaving limited downtime for installing updates. In addition, some software patches must be validated by vendors or regulatory bodies before deployment to avoid invalidating service agreements or altering device functionality. Fortunately, the U.S. FDA [36] has clarified that new clearance is not required for security updates that do not affect a device's core functions [37], allowing healthcare organizations to address vulnerabilities more efficiently.

Best practices include scheduling patches during predetermined maintenance windows, testing them in controlled sandbox environments, and creating rollback plans in case an update introduces system instability. Ensuring good communication between radiology teams, information technology (IT) personnel, and third-party vendors is also vital so that each party understands the patch's scope, the potential impact on imaging operations, and the fallback measures if difficulties arise.

**Data backup and recovery**—Even with robust security measures in place, radiology departments must plan for the possibility that an attack could succeed. Swift recovery from data loss or encryption is therefore critical. A hospital system's resiliency after a cyberattack is proportional to its data backup strategy [38]. By extension, offline and redundant backups of imaging data and radiology information systems can be effective countermeasures to ransomware, allowing departments to restore operations regardless of their decision to pay.

A widely endorsed framework is the “3-2-1” backup strategy [39]: three copies of data; two distinct storage media, such as a local network storage device and a separate removable or cloud-based medium; one offsite or offline backup, to avoid simultaneous compromise of all copies. To further safeguard patient information, encryption of both primary and backup data is recommended, particularly for offsite or cloud-based storage solutions.

A well-tested backup-and-restore process can significantly reduce operational downtime after a disabling event [40]. Simulating recovery efforts is important, and both technically valid backups and the operational expertise to execute restoration are essential. These drills can expose hidden vulnerabilities, including incomplete file versioning or undocumented restoration procedures. A thoughtful data restoration strategy for workstations and servers provides benefits beyond ransomware recovery. For example, robust backup and recovery plans enabled some hospital systems to resume operations within hours after a widespread system outage caused by a 2024 CrowdStrike security update [41].

## Human Factors

*Employee training and awareness*—Even the most sophisticated technical controls can be undermined if staff mistakenly open phishing emails or unintentionally disable security features. Ongoing cybersecurity education for technologists, radiologists, administrative staff, and trainees is therefore essential. In a study reviewing reportable data breaches affecting 500 or more patients between 2015 and 2020, unintentional actions and carelessness were responsible for 103 million compromised patient records, with phishing alone accounting for 93 million [42]. Although the proportions may have changed after the malicious Change Healthcare cyberattack [43], human factors remain a critical vulnerability.

A common first line of defense is awareness training focused on phishing detection, teaching personnel to scrutinize unexpected email links, attachments, or requests for credentials. Training should also include guidance on password hygiene, safe handling of portable media (e.g., USB drives), and the importance of promptly reporting suspicious network behavior [32]. When hospital staff members are well-informed, they are more likely to take appropriate action before malware spreads extensively [33,40].

*Tabletop simulations*—While training raises awareness, tabletop simulations help refine an organization’s incident response capabilities [44]. These exercises bring together relevant stakeholders, including radiologists, technologists, IT professionals, and administrative leaders, for a guided walk-through of a hypothetical breach scenario. Participants discuss and practice, step-by-step, how they would apply existing policies and procedures to detect the incident, coordinate a response, restore affected systems, and communicate with staff, patients, and external authorities [44]. Through tabletop simulations, organizations often discover overlooked details in their incident response plan.

In some cases, radiology departments might integrate parallel simulations alongside normal clinical operations [45]. For example, while standard imaging workflows continues, key personnel simultaneously practice the downtime workflow by manually documenting, verifying patient data on paper, and communicating contingencies via phone or other analog backups. This parallel approach helps staff maintain familiarity with offline workflows, which may be essential if a cyberattack disables digital systems. It also helps to identify potential bottlenecks, such as limited capacity to print large numbers of images or read them on alternative equipment. Organizations also may discover overlooked details including inconsistent contact lists, insufficient cross-training for key roles, or lack of a formal escalation pathway for deciding whether to disable certain network segments during an attack. By identifying and remediating these gaps proactively, radiology teams mitigate potential chaos during an actual crisis.

## Surviving an Attack

Surviving a cyberattack involves a staged cross-disciplinary response that evolves from immediate detection to long-term recovery. Figure 1 summarizes the sequential phases and key decision points in radiology's role during a cybersecurity incident.

### *Detection and Immediate Response*

The earliest clue of a cyberattack often comes from frontline staff who notice unusual behavior on their workstations. Suspicious activity (e.g., encrypted files or pop-up ransom notes) must be promptly reported to the IT helpdesk. Once a cyberattack is confirmed, swift action is critical. Affected radiology systems should be isolated from the network to prevent lateral spread of malware. Simultaneously, the radiology department must activate its incident response plan, alerting the institutional cybersecurity team and leadership.

Patient safety is uniformly a top priority during cyberattacks, but especially at the onset when uncertainty is the greatest. Ongoing scans or interventions must be managed carefully, and contingency workflows should be activated. In the initial response phase, the focus should shift to acute patient care, clear incident communication, and emergency downtime imaging operations [40]. Incoming patients typically remain unaware that a cybersecurity incident is unfolding. Front desk staff, technologists, and radiologists may initially rely on partial systems or cached patient information to proceed with urgent imaging. Uncompromised devices may work temporarily, but active connections risk spreading malware. During this interim period, the department must triage imaging, prioritize emergent studies over elective examinations, and seek alternatives for affected modalities.

Establishing a predefined incident command structure is critical. Key roles (e.g., incident commander, clinical liaison, departmental leads) coordinate resources and communications. Internal communication should be rapid via phone trees or secure messaging, with regular leadership updates on system status, isolation instructions, and access to paper-based resources. Externally, the hospital's public relations or communications team should manage messaging for patients, families, and media outlets, emphasizing that patient safety remains the top priority.

### *Containment and Mitigation*

Once the radiology department recognizes that multiple endpoints are compromised, the situation escalates to a major incident. Containment is often divided into two phases: the hyperacute phase, focused on immediate stabilization through assessment and damage control, and the acute phase, during which the organization switches to analog or limited digital resources to maintain business continuity.

IT teams may sever network connections and isolate systems to stop malware spread—disconnecting devices, shutting down segments, and revoking access. For example, during two 2020 hospital cyberattacks, IT teams proactively placed the EHR offline to prevent malware propagation [40,46]. Radiology IT systems such as PACS and scanner consoles may be disconnected from interhospital networks or the Internet until deemed secure. This abrupt isolation can cause significant operational disruption. Because radiology relies heavily on cross-departmental data exchange, immediate challenges may arise in retrieving prior studies, verifying patient identity, and communicating with referring clinicians. A pre-established downtime manual can support radiology staff by outlining whom to contact, what to shut down, and how to transition to backup systems [40].

The combination of the shutdown of compromised infected systems and defensive isolation of network connections makes the extent of downtime immediately apparent to most employees. Nursing units may lose access to electronic patient records, while scheduling offices may be unable to retrieve appointment information. During an attack's initial hours, the source and method of attack are often unclear. At this stage, hospital cybersecurity experts and external consultants are typically engaged. Specialized incident response teams can assist with forensic analysis to determine the attack vector, such as a phishing email, and locate malware and perpetrator footholds. The incident response lead should involve the institution's legal counsel and compliance officers early to navigate breach notification requirements and coordinate with law enforcement. Evidence, including log files and affected hardware, should be forensically preserved for investigation. While frontline informatics staff may be inclined to reimaging workstations immediately, law enforcement will usually advise retaining the compromised hardware for evidence and forensic review [47]. Investigators may recommend not to shut down compromised systems so that processes running in memory can be examined. It is therefore usually advised to disconnect these systems from the network to prevent spread

of malware while preserving forensic evidence on the device suspected of being compromised.

The acute phase of recovery starts at the point at which an organization recognizes that immediate full restoration is not possible and shifts to a prolonged downtime workflow [40]. In radiology, where imaging results are often time-sensitive, maintaining continuity of care is critical during this phase. Once leadership determines that digital workflows are compromised, the next urgent priority is switching to an analog or limited digital contingency plan. Paper-based order forms, manual scheduling logs, and verbal patient verification operating procedures can be activated if prepared in advance. In these situations, relevant imaging protocols are communicated by paper documents or direct communication. Portable ultrasound or digital radiography units that remain unaffected may continue to operate, although without standard electronic archival workflows.

## Post-Attack Recovery

### *Technology Recovery*

Recovery efforts begin with a forensic examination of affected devices and servers to determine the malware's nature and scope. Recovery generally proceeds in three phases: eradication of the malware, system restoration, and validation and testing to ensure data integrity and functionality. For most workstations that do not store unique data, eradication typically involves disinfecting, reformatting, or re-imaging machines. These methods are effective regardless of how much of the underlying software has been encrypted. Throughout this process, maintaining forensic evidence may be necessary for legal or insurance purposes. For digital assets that serve as a source of truth, including the EHR or PACS, data restoration must also be considered. If restoration from an offline or remote backup is planned, the hardware may be sanitized through reimaging. In cases where a data decryption key is acquired, the server may be digitally quarantined so that data can be restored, extracted, and transferred to refreshed hardware. Although most healthcare data are text-based and not executable, the DICOM standard allows small amounts of executable code, posing unique security considerations [24].

Once the environment is deemed secure, system restoration proceeds in a controlled stepwise manner. Mission-critical servers, such as those hosting the EHR or PACS, are prioritized. In parallel, archived images may be restored from backups to ensure continuity of imaging history. This process is most effective when supported by regular backup validation and strict version control, which reduce the risk of corrupted or incomplete restorations [40,48].

After restoration is complete, validation and testing are essential. Radiology and IT staff must verify the recovered data's integrity by testing sample patient records, reviewing archived images, and confirming proper function of core systems such as scheduling and

reporting. Any residual anomalies must be addressed before clinical operations fully resume.

### *Data*

As the organization transitions from crisis response to recovery, a final and critical step is reconciliation of the interim paper-based records with the restored digital environment. This process requires meticulous attention, as any mismatch in patient information or imaging results can compromise patient safety. It is important to create reconciliation teams that include both IT support staff and clinical users [40]. These teams manually input paper records into the appropriate digital systems, verifying accuracy and adjudicating whether or not to exclude incomplete or mislabeled records.

Once the backlog of paper records has been integrated, radiology can resume a fully digital workflow. The post-incident phase also offers a key opportunity for institutional learning and improvement. Institutions commonly conduct a formal after-action review to identify successes and gaps, and guide future cybersecurity enhancements.

## **The Future: Emerging Technologies**

Artificial intelligence (AI) has become a transformative technology in radiology [49]. As its use expands, it is essential to understand the cybersecurity implications that accompany AI integration into healthcare systems [50].

AI algorithms are increasingly used to assist radiologists in interpreting medical images. These models are trained on large datasets drawn from multiple institutions, making preservation of data confidentiality a key concern. Federated learning offers one potential solution [51]. In this approach, AI models are trained locally on institutional data, and only the trained models, without PHI, are shared externally, preserving data privacy.

In addition to confidentiality, training data integrity must also be protected. Adversarial attacks, in which malicious actors manipulate input data to mislead AI models, can have significant consequences in the context of medical imaging [52]. Incorrect outputs may directly affect patient care. Transparent AI models that provide interpretable outputs can help detect when a system has been trained on flawed or tampered data [53].

Finally, cybercriminals can weaponize AI, particularly for advanced phishing and social engineering campaigns targeting healthcare personnel [54] (Table 2).

Other emerging technologies, such as blockchain, commonly used in the banking sector, can ensure data integrity, and have the potential to enhance security of medical data [55]. Use of blockchain technology may help to secure patient-controlled image sharing,

facilitate multiinstitutional research, and integrate AI across the medical imaging enterprise.

## Consensus Statements

- Cybersecurity is a foundational component of modern healthcare that requires urgent and sustained attention. Protecting the confidentiality, integrity, and availability of patient data and medical systems is essential to maintaining trust, service continuity, and patient safety amid escalating cyberthreats.
- Healthcare organizations face persistent and evolving cyberthreats, including data breaches, phishing, ransomware, and social engineering. These pose serious risks to patient safety, institutional integrity, and regulatory compliance.
- Radiology departments are particularly vulnerable to cyberattacks due to their dependence on often legacy and insecure digital imaging systems, as well as a reliance on network connectivity and specialized software. As a result, radiology departments are critical points of risk within healthcare institutions.
- Human factors, including inadequate training, susceptibility to phishing, and limited cybersecurity awareness among staff, remain a primary entry point for many cyber-incidents in healthcare. Cybersecurity training should be tailored to all medical personnel and emphasize phishing recognition, password hygiene, and safe digital practices.
- Radiology practices must adopt a layered cybersecurity approach informed by risk assessment and threat modeling. These insights should inform a defense-in-depth strategy incorporating physical, technical, and administrative safeguards aligned with HIPAA and other regulatory standards.
- Cybersecurity measures must include prevention, detection, resilience, and recovery planning to ensure continuity of care and reduce the impact of inevitable cyber-incidents.
- Early detection and rapid isolation are critical to limiting the damage caused by cyberattacks. Frontline staff play a vital role in recognizing suspicious behavior. Once a cyberattack is suspected, affected systems must be promptly reported and disconnected from the network to contain the spread of malware and safeguard patients.
- An organized predetermined incident response structure is essential for effective crisis management. Activating a formal incident command system that includes IT

leaders, clinical liaisons, and department heads ensures clear communication, prioritization of critical services, and coordinated resource deployment during the acute phase of an attack.

- Comprehensive post-attack recovery includes secure system restoration, data reconciliation, and institutional learning. Once systems are disinfected and restored, detailed validation ensures data integrity, while dedicated teams reconcile paper-based records. A structured after-action review identifies lessons and enhances future cyber resilience.
- The integration of artificial intelligence into radiology holds great promise for enhancing diagnostic accuracy and efficiency but must be accompanied by robust cybersecurity strategies. These include preserving data confidentiality through federated learning and protecting data integrity against adversarial attacks.

## References

1. Nguyen XV, Petscavage-Thomas JM, Straus CM, Ikuta I. Cybersecurity in radiology: Cautionary Tales, Proactive Prevention, and What to do When You Get Hacked. *Current Problems in Diagnostic Radiology*. Vol 54, Issue 2, March–April 2025, Pages 245-250.
2. Balasubramanian S. With Increasing Reliance On Healthcare Technology, Cybersecurity Is A Growing Concern. *Forbes*, Apr 29, 2023. Available at: <https://www.forbes.com/sites/saibala/2023/04/29/with-increasing-reliance-on-healthcare-technology-cybersecurity-is-a-growing-concern/>, Accessed on: May 25 2025.
3. What Is The CIA Triad? Available at: <https://www.fortinet.com/resources/cyberglossary/cia-triad>, Accessed on May 24 2025.
4. Miliard, M. Hospital ransomware attack led to infant's death, lawsuit alleges. *Healthcare IT News*. October 01, 2021. Available at: <https://www.healthcareitnews.com/news/hospital-ransomware-attack-led-infants-death-lawsuit-alleges>, Accessed on: May 25 2025.
5. HHS. Health Insurance Portability and Accountability Act of 1996 Public Law 104-191 Available at: <https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996>. 1996. Accessed on: May 24, 2025.
6. Alder, S: "Healthcare Data Breach Statistics", May 18, 2025, Available at: <https://www.hipaajournal.com/healthcare-data-breach-statistics/>, Accessed on: May 24, 2025.
7. Rosch, F. One Year Later: Cybersecurity Lessons From Change Healthcare Breach. *Forbes*, Apr 1 2025. Available at: <https://www.forbes.com/councils/forbestechcouncil/2025/04/01/one-year-later-cybersecurity-lessons-from-change-healthcare-breach/>, Accessed on: May 25 2025.

8. 2024 State of the Phish – Today’s Cyber Threats and Phishing Protection. Proofpoint. 2024. Available at: <https://www.proofpoint.com/us/resources/threat-reports/state-of-phish>, Accessed on: May 25 2025.
9. Riley, C, Insurance giant Anthem hit by massive data breach. CNN Business, February 6 2025. Available at: <https://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/>, Accessed on: May 25 2025.
10. Kolbasuk McGee, M. Malware Leads to Health Data Breach. Patients at University of Washington Medicine Affected. Data Breach Today, December 3 2025. Available at: <https://www.databreachtoday.com/malware-leads-to-health-data-breach-a-6258>, Accessed on: May 25 2025.
11. Sjouwerman, Stu. 91% of cyberattacks begin with spear phishing email. <https://blog.knowbe4.com/bid/252429/91-of-cyberattacks-begin-with-spear-phishing-email>. Accessed Jun 27, 2025.
12. “Spear Phishing”, Trend Micro, Available at: <https://www.trendmicro.com/vinfo/us/security/definition/spear-phishing>. Accessed on: May 25 2025.
13. Prümmer J, van Steen T, van den Berg B. A systematic review of current cybersecurity training methods. *Computers & Security*, Vol 136, January 2024, 103585.
14. Proofpoint. Measuring Up: Metrics, Benchmarks, and Communicating Security Awareness Training Success. <https://www.proofpoint.com/uk/blog/security-awareness-training/measuring-metrics-benchmarks-and-communicating-security-awareness>. Accessed Jun 27, 2025.
15. Sophos, The state of Ransomware 2024, Available at: <https://www.sophos.com/en-us/content/state-of-ransomware>, Accessed on: May 25 2025.
16. Irei, A. 2024. Tech Target “Top 10 ransomware targets by industry”. April 24 2025. Available at: <https://www.techtarget.com/searchsecurity/feature/Top-10-ransomware-targets-in-2021-and-beyond>, Accessed on: 25 May 2025.
17. Weiner, S. The growing threat of ransomware attacks on hospitals. *AAMC News*. July 20, 2021. Available at: <https://www.aamc.org/news/growing-threat-ransomware-attacks-hospitals>, Accessed on: May 25 2025.
18. Muoio D. Rural Illinois hospital says 2021 ransomware attack partially to blame for closure. *Fierce healthcare*, Jun 13, 2023. Available at: <https://www.fiercehealthcare.com/health-tech/rural-illinois-hospital-says-shutdown-partially-caused-2021-ransomware-attack>, Accessed on: May 25 2025.
19. “Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients”. Available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4579292](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4579292), accessed on: May 25 2025.
20. Carpenter P. Ransomware: Five Reasons Why Victim Organizations Pay Up. *Forbes*. Jul 09, 2021. Available at: <https://www.forbes.com/councils/forbesbusinesscouncil/2021/07/09/ransomware-five-reasons-why-victim-organizations-pay-up/>, Accessed on: May 25 2025.
21. Ransomware Double-Dip: Re-Victimization in Cyber Extortion. *The Hacker News*. Apr 22, 2024. Available at: <https://thehackernews.com/2024/04/ransomware-double-dip-re-victimization.html>, Accessed on: May 25 2025.

22. Winder, Davey. (2021) Forbes Ransomware Reality Shock: 92% Who Pay Don't Get Their Data Back. Forbes. Last updated Jun 29, 2021, 04:48am EDT. <https://www.forbes.com/sites/daveywinder/2021/05/02/ransomware-reality-shock-92-who-pay-dont-get-their-data-back/> Accessed Jun 27, 2025.
23. Eichelberg M, Kleber K, Kämmerer M. Cybersecurity Protection for PACS and Medical Imaging: Deployment Considerations and Practical Problems. *Academic Radiology*, Vol 28, Issue 12, p1761-1774, December 2021.
24. Desjardins B, Mirsky Y, Ortiz MP, et al. DICOM Images Have Been Hacked! Now What? *AJR Am J Roentgenol*. 2020;214(4):727–35.
25. Alder S. 400 Million Medical Images Are Freely Accessible Online Via Unsecured PACS. *HIPAA Journal*. Sept 18 2019. Available at: <https://www.hipaajournal.com/400-million-medical-images-are-freely-accessible-online-via-unsecured-pacs/>, Accessed on: May 25 2025.
26. Adler S. Update Issued on Unsecured PACS as Exposed Medical Image Total Rises to 1.19 Billion, Nov 18, 2019. Available at: <https://www.hipaajournal.com/update-issued-on-unsecured-pacs-as-exposed-medical-image-total-rises-to-1-19-billion/>, Accessed on: May 24, 2025.
27. Amri A, Molige S, dos Santos D. Healthcare Malware Hunt, Part 1: Silver Fox APT Targets Philips DICOM Viewers. February 24, 2025. Available at: <https://www.forescout.com/blog/healthcare-malware-hunt-part-1-silver-fox-apt-targets-philips-dicom-viewers/>, Accessed on: May 24, 2025.
28. Mirsky Y, Mahler T, Shelef I, Elovici Y. CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning, arXiv:1901.03597. April 3, 2019. Available at: <https://arxiv.org/abs/1901.03597>, Accessed on: May 24, 2025.
29. Picado Ortiz M. Weaponized Medical Images: Is Malware Hiding in Your MRI Results?, April 27, 2019. Available at: <https://labs.cylera.com/2019/04/16/pe-dicom-medical-malware/>, Accessed on: May 24, 2025.
30. Enzmann DR. Radiology's Value Chain. *Radiology*. 2012 Apr;263(1):243–52.
31. United States Health and Human Services. The HIPAA Security Rule [Internet]. Available at: <https://www.hhs.gov/hipaa/for-professionals/security/index.html>, Accessed on: May 25 2025.
32. Andriole KP. Security of Electronic Medical Information and Patient Privacy: What You Need to Know. *J Am Coll Radiol*. 2014 Dec;11(12):1212–6.
33. Palanivel M, Selvadurai K. Risk-driven security testing using risk analysis with threat modeling approach. *SpringerPlus*. 2014;3:754.
34. Industrial Control Systems Cyber Emergency Response Team. Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies [Internet]. 2016. Available at: [https://www.cisa.gov/sites/default/files/recommended\\_practices/NCCIC\\_ICSCERT\\_Defense\\_in\\_Depth\\_2016\\_S508C.pdf](https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICSCERT_Defense_in_Depth_2016_S508C.pdf), Accessed on: May 25 2025.
35. Dhiman P, Saini N, Gulzar Y, et al. A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model. *Sensors (Basel)*. 2024 Feb 19;24(4):1328.
36. Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, September 2023. Available at:

- <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-system-considerations-and-content-premarket-submissions>, Accessed on: May 25 2025.
37. Information for Healthcare Organizations about FDA's "Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-The-Shelf (OTS) Software" [Internet]. U.S. Food and Drug Administration; 2005 Feb. Available at: <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/information-healthcare-organizations-about-fdas-guidance-industry-cybersecurity-networked-medical>, Accessed on: May 25 2025.
  38. Ghayoomi H, Laskey K, Miller-Hooks E, Hooks C, Tariverdi M. Assessing resilience of hospitals to cyberattack. *Digit Health*. 2021;7:20552076211059366.
  39. Perkel JM. 11 ways to avert a data-storage disaster. *Nature*. 2019 Apr 4;568(7750):131–2.
  40. Chen PH, Bodak R, Gandhi NS. Ransomware Recovery and Imaging Operations: Lessons Learned and Planning Considerations. *J Digit Imaging*. 2021 Jun;34(3):731–40.
  41. Wicklund E. Healthcare Takes a Breath After CrowdStrike Scare. *PSQH*, July 22, 2024. Available at: <https://www.psqh.com/news/healthcare-takes-a-breath-after-crowdstrike-scare/>, Accessed on: May 25 2025.
  42. Yeo LH, Banfield J. Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. *Perspect Health Inf Manag*. 2022;19(Spring):1i.
  43. Kerner SM. The Change Healthcare attack: Explaining how it happened. *Techtarget*. 08 Mar 2024. Available at: <https://www.techtarget.com/WhatIs/feature/The-Change-Healthcare-attack-Explaining-how-it-happened>, Accessed on: May 25 2025.
  44. Maggio LA, Dameff C, Kanter SL, Woods B, Tully J. Cybersecurity Challenges and the Academic Health Center: An Interactive Tabletop Simulation for Executives. *Acad Med J Assoc Am Med Coll*. 2020 Nov 24.
  45. Dhamija A, Moskovitz JA, Regan J, et al. PACS downtime drill: testing departmental workflow with an enterprise imaging viewer and archive. *Pediatr Radiol*. 2022 Jun;52(7):1234-1241.
  46. Reeves K. Cyberattacks: Not a Matter of If, but When. [cited 2025 Feb 10]; Available at: <https://appliedradiology.com/Articles/cyberattacks-not-a-matter-of-if-but-when>, Accessed on: May 25 2025.
  47. Federal Bureau of Investigation. FBI Guidance to Victims of Cyber Incidents on SEC Reporting Requirements.
  48. Ruggiero P, Heckathorn MA. Data Backup Options [Internet]. United States Computer Emergency Readiness Team; 2012. Available at: [https://www.cisa.gov/sites/default/files/publications/data\\_backup\\_options.pdf](https://www.cisa.gov/sites/default/files/publications/data_backup_options.pdf), Accessed on: May 25 2025.
  49. The Impact of Artificial Intelligence in Radiology. Eltorai AEM (Editor), Guo HH (Editor), CRC Press, Dec 27 2024, 240 p.
  50. Shah C, Nachand D, Wald C, Chen PH. Keeping Patient Data Secure in the Age of Radiology Artificial Intelligence: Cybersecurity Considerations and Future Directions. *Journal of the American College of Radiology*. 2023 Sep;20(9):828–35.

51. Yin X, Zhu Y, Hu J. A comprehensive survey of privacy-preserving federated learning: A taxonomy, review, and future directions. *ACM Comput. Surv.* 2021; 54:1–36.
52. Sorin V, Soffer S, Glicksberg BS, Barash Y, Konen E, Klang E. Adversarial attacks in radiology – A systematic review. *European Journal of Radiology*, Volume 167, 111085, October 2023.
53. Saranya A, Subhashini R. A systematic review of Explainable Artificial Intelligence models and applications: Recent developments and future trends. *Decision Analytics Journal*, Vol 7, June 2023, 100230.
54. Elliott, D. Lessons learned from a \$25m deepfake crime, *World Economic Forum*, Feb 4, 2025. Available at: <https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/>, Accessed on: May 25 2025.
55. Tomihama RT, Wilkinson MC, Kiang RC. Blockchain Technology: Overview and Applications in Radiology. *American Journal of Roentgenology*, In Press, 2025.

ACCEPTED  
MANUSCRIPT

Table 1: Definitions of Types of Cyberattacks

Term	Definition	Potential Impact on Radiology Department
Unauthorized access	When an individual gains access to a computer, network, or data without permission. It can occur through exploiting software vulnerabilities, stealing credentials, or bypassing security measures.	Data breaches, unauthorized image tampering, and exposure of sensitive patient information. Compliance violation. Needs to be investigated to uncover what PHI was compromised or to prove that no PHI was accessed.
Insider threat	A security risk originating from within the organization, such as employees or contractors, who may intentionally or unintentionally cause harm.	PHI or IP data may be stolen and copied to portable media or malicious software uploaded to trusted systems for later ransomware or other attack. May lead to data breaches, unauthorized access to imaging systems, or unintentional security lapses affecting patient data integrity and ultimately patient safety.
Denial of service	Attack that aims to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. This aim is often achieved by overwhelming the target with a flood of incoming traffic.	Prevents radiology devices from connecting to the network, disrupting workflows, delaying critical imaging procedures, and potentially leading to patient care delays.
Buffer overflow	When a program or process attempts to write more data to a fixed-length block of memory, or buffer, than it is allocated to hold. This occurrence can corrupt data, crash the system, or allow the execution of malicious code.	Can cause system crashes or unauthorized code execution, leading to service disruption, data loss, or corruption, directly affecting patient care and data integrity.
Phishing attacks	A form of fraud where fraudulent emails or copycat websites are used to trick individuals into	May result in unauthorized access, data breaches, and introduction of malware into the

	revealing personal information, such as passwords, credit card numbers, or Social Security numbers. Phishing often lays the foundation for further cyber-attacks. Spear phishing and whaling are variants that refer to phishing attacks on a high-yield target organization or person.	radiology network, undermining system integrity, patient confidentiality, and, ultimately, patient safety.
Malware	Malicious software designed to disrupt, damage, or gain unauthorized access to systems.	May infiltrate radiology systems through infected attachments or downloads, leading to data loss, theft, downtime, or patient safety concerns.
Social engineering	Psychologic manipulation used by attackers to trick individuals into revealing confidential information or performing actions that compromise security.	Can lead to unauthorized access or malware introduction, especially when staff are tricked into clicking links, sharing passwords, or bypassing protocols.
Ransomware	A type of malicious software designed to block access to a computer system until a sum of money is paid. Once a system is infected, ransomware encrypts files and demands payment, typically in cryptocurrency, for decryption keys.	Can lead to significant downtime, data loss, and potential breach of patient confidentiality if the attack is not managed properly, along with financial losses.
Multi-extortion ransomware	A ransomware attack that not only encrypts data but exfiltrates PHI and threatens to release it publicly unless a ransom is paid.	Increases pressure to pay ransom and adds reputational risk, regulatory exposure, and privacy concerns. Known as secondary or tertiary cyber extortion.
Deepfake	Synthetic audio or video media created using AI to impersonate real individuals for malicious purposes.	May be used in phishing or impersonation schemes to deceive staff into making financial or operational decisions.
Software vulnerabilities	Flaws or weaknesses in a software program or system that can be exploited by cyber-attackers to gain unauthorized access or cause other harmful actions to the system.	Increases the risk of attacks that can disrupt imaging operations or lead to data breaches, affecting the overall security and reliability of radiologic services.

Advanced persistent threat	A prolonged and targeted cyberattack where an intruder gains access and remains undetected to steal data or compromise systems.	Can allow undetected backdoor access to PACS or DICOM viewers, enabling long-term data theft or image manipulation.
Physical security breaches	Unauthorized physical access to an organization's buildings, equipment, or data storage locations. This type of breach can include actions like theft, vandalism, or unauthorized entry.	May result in theft or tampering of hardware and data, impacting patient privacy and service continuity and potentially leading to regulatory and compliance issues.
Cyber assassination	Compromise of clinical systems results in gain of access by perpetrators to critical control systems for malicious manipulation.	May result in a patient receiving wrong or lethal doses of radiation.

PHI = protected health information; IP = intellectual property; AI = artificial intelligence

ACCEPTED MANUSCRIPT

Table 2: Examples of High-Profile Cybersecurity Incidents

Incident Type	Incident Description
Third-party data breach	In 2024, Change HealthCare, a vendor providing data services to many healthcare organizations, experienced a ransomware attack that halted the processing of medical claims and electronic payments. The breach affected the medical information of 190 million patients. It paralyzed billing and insurance operations, delayed payments, and threatened the financial stability of numerous healthcare institutions. Affected hospitals reported losses totaling hundreds of millions of dollars [7].
Malicious link	In 2015, Anthem (previously known as Wellpoint), one of the largest health insurance companies in the United States, experienced a major data breach. The attack began with a phishing email containing a malicious link in which the word “Wellpoint” was replaced by “We11point,” a change that was difficult to detect with the font used in the email. Employees clicked the link, unknowingly downloading a keystroke-logging software that captured their login credentials and granted hackers access to the company’s network, ultimately exposing 78.8 million medical records [9].
Malicious attachment	In 2013, the University of Washington Medical Center was affected by a cyberattack after an employee of an affiliated entity opened a malicious email attachment on a laptop. The attachment, which appeared to be a routine administrative file, contained malware that took full control of the device and its data. The compromised laptop contained the medical records of more than 90,000 patients [10].
Ransomware attack	In 2020, United Health Services (UHS), one of the largest healthcare networks in the United States, experienced a ransomware attack that targeted IT systems, locking patient data and critical medical records. Staff were unable to access vital patient information and were forced to rely on paper records and manual processes to manage patient care. Hospitals nationwide were affected, resulting in canceled surgeries, delays in emergency care, and significant operational disruption [15].
Ransomware attack	In 2019, a ransomware attack on a hospital in Alabama led to a neonate’s death. A pregnant woman was admitted for delivery while the hospital’s networks were disrupted by a cyberattack. She was placed on a routine fetal monitoring system, which eventually detected fetal distress. However, the alert could not be transmitted to the nursing station due to the network outage. The fetus’s umbilical cord was wrapped around its neck, causing brain anoxia and, ultimately, death [4].
Deepfake	In 2024, a global engineering firm headquartered in England experienced a cyberattack using deepfake technology. During a routine video conference, attackers impersonated multiple senior hospital executives

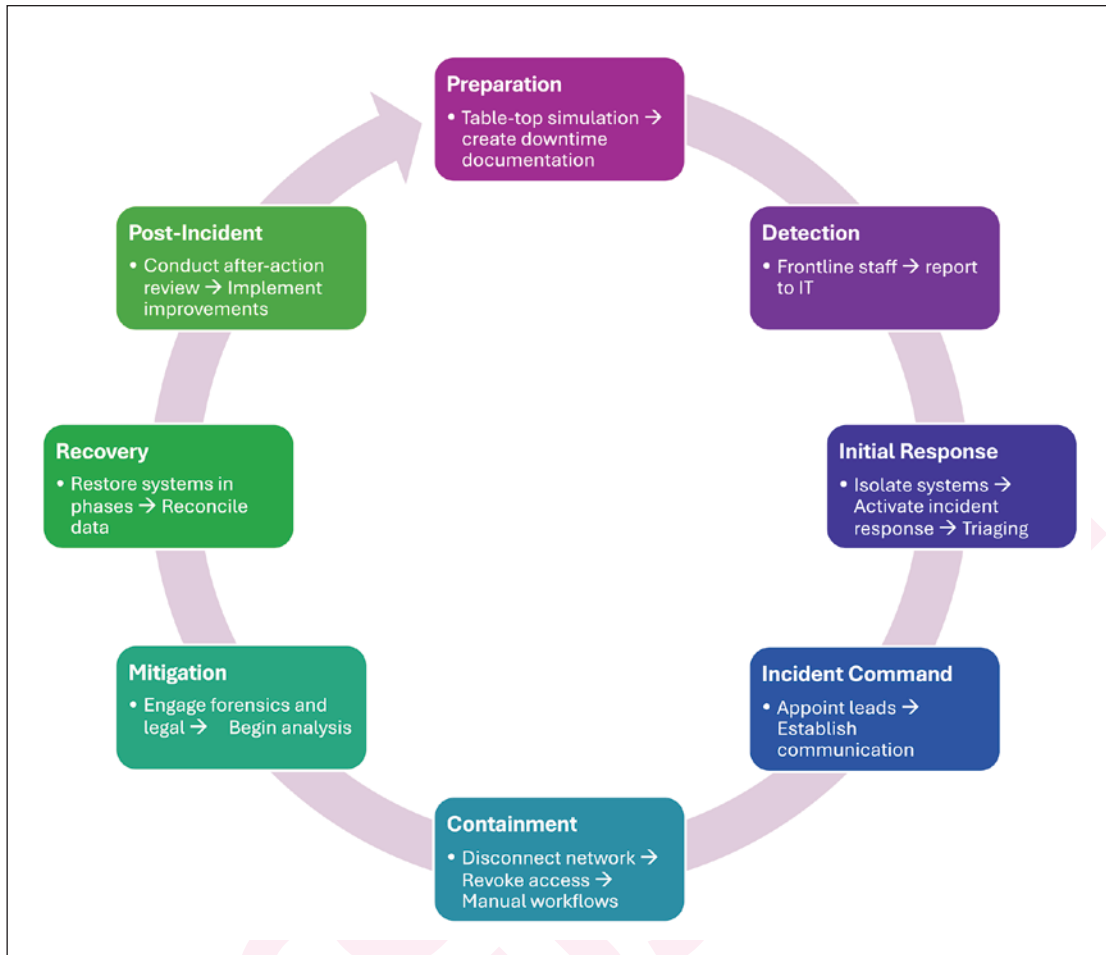
	by creating highly convincing deepfake videos of the executives' faces and voices. Under these false identities, they instructed a staff member to transfer approximately \$25 million to several bank accounts. Believing that the instructions were legitimate and not realizing that no other humans were in the video conference, the employee complied. The fraud was only discovered after the funds had been transferred [54].
--	---

ACCEPTED  
MANUSCRIPT

Table 3: Overview of Cybersecurity Readiness

<b>Focus</b>	<b>Activities and Components</b>
Risk assessment	
Hazard evaluation	Assessment of vulnerable assets, determination of likelihood and impact of attacks, implementation of safeguards
Threat modeling	Examination of exploitable vulnerabilities, formulation of a defense-in-depth strategy
Cyber hygiene	
Updates and patching	Up-to-date software, controlled testing, rollback plans
Data backup and recovery	Offline redundant systems
Human factors	
Awareness training	Phishing detection, password hygiene, safe handling of media
Tabletop simulations	Refinement of incident response, discovery of overlooked details

ACCEPTED MANUSCRIPT



**Figure 1.** Radiology response phases during a cyberattack. IT = information technology

# How to Prepare for, Survive, and Recover From a Cybersecurity Attack: A Guide for Radiology Practices—AJR Expert Panel Narrative Review

## Authors:

### Corresponding:

**Benoit Desjardins, MD, PhD**

bdmdphd@me.com

Département de radiologie, radio-oncologie et médecine nucléaire

Centre Hospitalier de l'Université de Montréal (CHUM)

1051 Rue Sanguinet

Montréal, QC H2X 3E4, Canada

(514) 703-0050

@bdmdphd

Disclosures: None

### Other authors:

**Marla B.K. Sammer, MD, MHA**

mbsammer@texaschildrens.org

Singleton Department of Radiology

Texas Children's Hospital

6701 Fannin Street

Houston, TX 77030

(832) 824-7237

@MarlaSammer

Disclosures: None

**Alexander J. Towbin, MD**

Alexander.towbin@cchmc.org

Department of Radiology

Cincinnati Children's Hospital

3333 Burnet Ave MLC 5031

Cincinnati, OH 45229

(513) 636-5896

@towbinaj, @cincykidsrad

Disclosures: Research: Bayer; Consultant: Applied Radiology; Author Royalties: Elsevier

**Patricia Balthazar, MD, MPH**  
patricia.balthazar@emory.edu  
Department of Radiology & Imaging Sciences  
Emory University School of Medicine  
550 Peachtree Street Northeast  
Atlanta, GA 30308  
(404) 778-9729  
@PBalthazarMD  
Disclosures: None

**Richard Staynings, MS**  
richard@staynings.com  
Cylera  
140 Broadway, 46th Floor  
New York, NY, 10005  
(303) 601-8076  
@rstaynings  
Disclosures: Employee of Cylera

**Po-Hao Chen, MD, MBA**  
chenp2@ccf.org  
Imaging Institute  
Cleveland Clinic  
9500 Euclid Ave. Mail Code JJ36  
Cleveland, OH 44195  
(216) 445-6593  
@howardpchen  
Disclosures: None