Journal of Digital Imaging (2021) 34:731–740
https://doi.org/10.1007/s10278-021-00466-x

COMMENTARY

Ransomware Recovery and Imaging Operations: Lessons Learned and Planning Considerations

Po-Hao Chen[1,2,3] · **Robert Bodak**[2] · **Namita S. Gandhi**[1,3]

Received: 29 December 2020 / Revised: 5 May 2021 / Accepted: 17 May 2021 / Published online: 22 June 2021

Abstract
In this era, almost all healthcare workflows are digital and rely on robust institutional networks; a ransomware attack in a healthcare system can have catastrophic patient care consequences. The usual downtime processes in an institution might not address the breadth of this disruption and timelines for recovery. This article shares our lessons learned from ransomware recovery. From this experience, a four-phase recovery planning framework has been developed. The primary focus is on acute patient care, incident communication, and emergency imaging operations in the initial phase. In the next phase, continued digital asset unavailability necessitates a transition to long-term analog workflows. In the infrastructure recovery and reconciliation phases, each taking weeks or months, the emphasis is on rebuilding a ransomware-free environment and reconciling the data accrued during extended downtime. In preparation for future events, we have initiated a continuous readiness process. A response task force has been formed to guide physicians, technologists, nurses, and informatics units on recovery workflows appropriate for extended downtime and keeping these procedures updated. Incident command structure has been discussed for communications and resource allocation during a ransomware attack, possibly in the context of a multi-incident scenario such as that involving concurrent staffing shortage amidst a pandemic. Finally, we discuss considerations for tabletop simulation, which may be valuable to the planning process.

Keywords Cybersecurity · Ransomware · Disaster recovery · Radiology operations · Business continuity

Introduction

Earlier in 2020, one of the hospitals within our institution's tertiary referral network was the target of a ransomware attack. The facility's radiology caregivers were forced to switch to a paper-based workflow, using written orders, reports, and CD/DVD to store diagnostic images to achieve operational recovery. The ensuing months proved that it was one in a series of increasingly prevalent cybersecurity threats targeting healthcare systems across the USA. In the same month, larger health systems also reported ransomware attacks that crippled hundreds of healthcare systems.

✉ Po-Hao Chen
chenp2@ccf.org

[1] Department of Diagnostic Radiology, Imaging Institute, Cleveland Clinic, 9500 Euclid Avenue, Cleveland, OH, USA

[2] Section of Imaging Informatics, Imaging Institute, Cleveland Clinic, 9500 Euclid Avenue, Cleveland, OH, USA

[3] Information Technology Division, Cleveland Clinic, 9500 Euclid Avenue, Cleveland, OH, USA

For these reasons, when an advisory from the Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency (CISA), and the Department of Health and Human Services raised a joint national alert regarding ransomware threats targeting hospital systems across the country, many health systems began taking serious steps to address them [1]. CISA also regularly issues medical device advisories, identifying security loopholes that can provide a vector for data theft or ransomware, more recently finding such vulnerabilities that affect over 100 devices including radiography, CT, MRI, US, mammography, PET, interventional, and others [2].

Our US-based radiology and nuclear medicine practice consist of over 200 radiologists across two US states, performing approximately 2.5–3 million radiology examinations yearly in a combination of academic, community-based, and remote practices. While our first experience with ransomware attack recovery affected but a small fraction of the caregivers and patients in the network, the extent of workflow modifications necessary to sustain operations was substantial. When the ransomware attack was triggered

involving a small hospital within our network, some computing assets were disabled immediately by the ransomware. An early defensive mechanism from our information technology (IT) department quickly disconnected the afflicted hospital from the remainder of the Enterprise network. The combined effect of the ransomware attack and the ensuing defense limited the impact and damage, but it also rendered nonfunctional the workflows that rely on operational networks and computers (as described below, this experience would inform much of "phase 1" planning). The emergency department was initially placed on diversion, and elective procedures and appointments were rescheduled. Within radiology over the ensuing days to weeks, technologists, imaging informatics professionals, nurses, and radiologists worked jointly to develop a series of analog solutions for imaging operations using paper and plastic.

Knowing that the malware could have caused much more damage had it affected the entire system, we began extensive cybersecurity planning for the hospital system. While proper preparation requires detailed prevention, containment, and recovery planning, we find that a paucity of literature exists specifically addressing business continuity and recovery planning in radiology operations. This manuscript discusses our approach to planning for radiology business continuity in a catastrophic ransomware attack.

Assumptions and Scope

Cybersecurity threat management in radiology departments is unique from other clinical departments in several ways. First, radiology consists of horizontal service lines spanning outpatient, inpatient, intensive care, emergency care, and intraoperative care. Therefore, operational recovery for radiology requires considerations for each clinical service it supports. Second, many radiology services have standalone IT infrastructures, and some even have dedicated independent IT teams.

Cybersecurity events vary widely in mechanics, extent, and impact. While some cybersecurity threats aim to exfiltrate sensitive data, others can seek to manipulate connected medical devices [3, 4]. In contrast, a targeted ransomware attack is unique in that the effect is an operational disruption. The primary goal is often to extort payments, but in some cases, such as in cyberterrorism, the cessation of hospital operation may be the primary endpoint. Upon successful penetration, the malware spreads throughout a healthcare organization's network—sometimes affecting both original and backup copies. The most common form of attack is by performing whole disk encryption of all assests by remote triggering, thereby disabling them. Perpetrators often ask the affected organization for payment in cryptocurrency, offering a decryption key in exchange. With critical service disruption, an organization may choose to comply.

Although cyberattack prevention and containment may be organized centrally by the Information and Technology Division (ITD), the purpose of this article is to discuss lessons learned from our experience in preparation for a future attack. We have realized that a ransomware attack poses unique challenges with the operational impact and recovery timescale compared to disaster contingency planning caused by standard downtime, which can occur with picture archive and communication system (PACS) or imaging archive [3]. Standardizing the assumptions is also critical, as planning from a heterogeneous starting point or planning for every conceivable scenario is infeasible or potentially dangerous.

First, we share the phase-based approach describing the natural progression of a ransomware attack's effect on operational demands and their associated planning considerations (Fig. 1). This framework was developed based on several sources: our experience recovering a radiology practice from ransomware, discussion with other affected organizations, and information from reliable published sources such as the US Cybersecurity and Infrastructure Security Agency [1, 5]. The second half of the article focuses on the approach our institute has taken these lessons learned to inform a recovery planning effort for the future.

Phase 1–Hyperacute ("First 48 Hours")

Although some malware has an incubation period, for recovery planning, we defined hour 0 as the first sign of operational impact. Like in acute stroke care, the exact hour of onset is often difficult to identify, but a time-based lens to recovery planning remains helpful. The earliest signs of a catastrophic event maybe that multiple IT systems have been affected at the same time. Our experience suggests that all internet and intranet access, associated applications including caregiver scheduling, paging system, and online phone directory, may be disabled either as protective measures to limit damage or be directly affected by malware. Disabled assets may include nearly all networked computer hardware, including diagnostic reading stations, workstations on the inpatient, outpatient, and emergency units. All patient data, including the EMR, PACS, and radiology information system (RIS), were assumed to be either inaccessible or permanently disabled. Some imaging modalities may be vulnerable, while others may be isolated from the standard hospital network, allowing for continued image acquisition, albeit without a working intranet for data transmission. Portable modalities were also assumed to be available in a similarly offline configuration. Phone lines remained open, but the availability of digital, voice-over-IP (VOIP) lines required

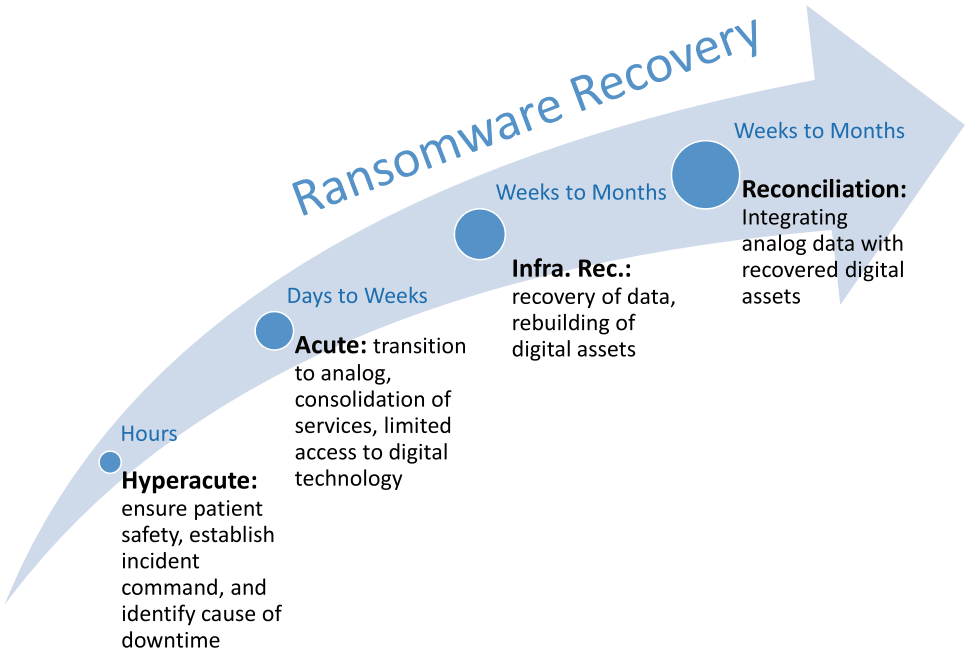

Fig. 1 Phases of ransomware recovery, noting that timing is approximate and varies based on size, complexity, and readiness of the imaging practice. Infra. Rec. = infrastructure recovery

a formal assessment by hospital Telecommunications. By extension, the analog functionalities of fax machines and photocopiers are assumed to be available but without advanced features requiring a digital connection.

However, the early hours of a ransomware attack can be indistinguishable from standard (short-term) network downtime for most caregivers. Therefore, in the hyperacute phase, a sudden mismatch between the supply and demand of imaging services ensues in at least three ways: first, patients continue to arrive at outpatient imaging centers, emergency department, and in urgent care facilities. Secondly, surgical patients may have intraoperative and peri-operative imaging demands at the time of impact. Finally, patients may be undergoing an image-guided procedure in an interventional, ultrasound, or CT suite when computers and offline medication dispensary devices become suddenly disabled, making it difficult to provide the needed care.

For these reasons, in the hyperacute phase, a radiology department would face operational demands from ongoing emergency services, active interventional procedures, and continued outpatient imaging. These demands must be managed without access to technology assets. It is also worth highlighting that the "48 h" is approximate and for planning only, as the transition from phase 1 to phase 2 can occur well before or after 2 days.

Planning Considerations for Phase 1

Response for Phase 1 should be focused on immediate patient safety and the assessment of initial damage. An urgent and emergency workflow that cannot be suspended must be switched to paper-based workflows. Initial availability assessment on imaging modalities by technologists, nursing, and radiologists on their respective technology assets must be performed, allowing the department to report its residual capabilities and capacity to a centralized response team such as an incident command center.

If clinical operation resumes during this phase, all imaging interpretation must be performed at the modality directly, with the knowledge that most modality-connected monitors are not of diagnostic quality. Any off-hour teleradiology coverage for emergency or urgent care must be considered unavailable and replaced with the at-modality review. Hub-and-spoke workflows where advanced examinations are performed in many imaging sites but interpreted centrally should be replaced by service suspension and consolidation to decrease the number of possible locations for imaging, as well as a distribution of radiologists to cover these sites. For smaller hospitals and independent facilities which do not have a radiologist on site, the radiology operations might have to be suspended, until there is a mechanism established to read off modalities. Patients with urgent or emergency indications may need to be diverted to facilities where some radiologist services remain available or diverted to an unafflicted hospital system. Communications with referring providers can still be performed by phone, but a downtime phone directory should be available.

A brisk initiation of downtime data reconciliation steps is necessary if emergency imaging services are to be sustained. For instance, emergency medication access for sedation is needed for ongoing procedures. Without access to the RIS and EMR, temporary conventions for the assignment of an imaging accession (defined by imaging informatics) and unique patient identifiers (defined centrally by the health

system) must be in place for diagnostic imaging. While these steps are often informal or unit-based in shorter downtime scenarios, the recovery from a catastrophic ransomware attack is often sufficiently long to enforce standardization.

Finally, the response must be coordinated both within radiology and the health system, preferably by establishing an incident command center following the National Incident Management System.

Phase 2—Acute ("First 3 Weeks")

After the first few days of downtime and the intense initial informatics efforts in diagnostic and recovery efforts, phase 2 begins with most radiology caregivers understanding the overall damage in their immediate setting. The hospital or health system's informatics team is assumed to have assessed the scale of damage, ranging from a subset of affected facilities to system-wide outage. As a response, some early executive decisions on service continuation and service diversion—either as part of consolidating services centrally or directing patients to other health systems—will have been made.

With proper recovery planning, it is reasonable to assume that some technology assets can be restored within the phase 2 timeframe. If the underlying EMR data is either unaffected or quickly recovered, limited access such as read-only access may be achieved. However, as the internal network connection, the enterprise directory, and affected end-user computers are disabled, access may be restricted to web-based versions and mobile versions of the application. In some cases, individual departments like radiology may have creative solutions towards purpose-specific technology using cellular internet, ad hoc networking, or offline computers. However, most of the system is likely to rely on a low-tech workflow using paper, fax, telephone, or traditional pager. Therefore, integration across departments for imaging exam ordering, patient scheduling, data transfer, and result communication would depend on an analog workflow.

Planning Considerations for Phase 2

Planning for phase 2 should be on persuing an end-to-end workflow focused on patient care at each step of the radiology value chain from the placement of orders to the communication of results. Proper business continuity considerations would include additional focuses on data consistency and analog archiving for eventual reconciliation with the digital system. Continued attention should be paid to the urgent and emergency imaging needs of the hospital services. Even if limited EMR access were available, a low threshold would need to be set for communicating by phone for many imaging orders if caregivers could not depend on it for fully up-to-date information on laboratory results and allergies.

Despite emerging cloud-based technology, most of the current radiology technology assets PACS, RIS, and dictation software require an internal network connection. Offline digital image viewing capabilities may be enabled through freshly imaged, offline computers connected to diagnostic-quality displays. An offline CD/DVD workflow may be used to perform the initial data transfer between the modality and reading stations.

Depending on the availability of informatics resources, the readiness of recovery preparation, and the size and complexity of the radiology practice and its associated imaging center, it may be feasible in some situations to set up an ad hoc radiology network connecting the modalities, temporary PACS, and reporting servers, and reading workstations. However, in our experience, such ad hoc digital technology requires some careful planning before deployment. One radiology-specific phase 2 risk is the data heterogeneity arising from having a mix of paper records and digital data (e.g., CD/DVDs and an ad hoc PACS storage). In our experience, the eventual data reconciliation (phase 4) can be substantially streamlined by an organized phase 2 designed to prevent patient mismatches or lost data, as the reconciliation may be only possible months after the initial ransomware attack.

One additional consideration is understanding that analog media created during this phase may post a future risk. Many CD/DVD creation tools include an executable image viewer, which may contain malware if sourced from an afflicted computer and should be avoided in favor of a preinstalled DICOM viewer known to be safe. The DICOM files may also harbor malicious code [6]. Like other media files such as JPEG or TIFF, DICOM files should never be run as executable binaries. Tools, such as the open-source solution DCMTK (https://dcmtk.org), may be used to zero the potentially executable DICOM preamble and any padding.

As the organization moves into phases 3 and 4, both potentially afflicted media and the computers used to view them should not be connected to a new network.

Phase 3—Infrastructure Recovery

Both phases 3 and 4 depend more heavily on the information technology (IT) divisions than the radiology operation planning. As such, they are also not mutually exclusive to the other phases: a radiology IT team can begin the recovery of infrastructures while providing adjunct support to the analog or semi-analog workflows established in the first two phases. They are included in this article for completeness, but detailed technical preparation is beyond the scope of this article.

Each of the critical databases, such as PACS, EMR, and RIS, has one of three possible fates in a ransomware attack. First, the databases could remain unaffected due to some component of a successful preventive measure. In this setting, operational disruption occurs strictly due to inaccessibility from disabled computers rather than actual data loss. In the second possibility, the database can be disabled but recovered, either from an offline backup that was unaffected by the attack or by paying the perpetrator for an access key to unlock the data. Finally, the data can be permanently lost. A perpetrator such as a cyberterrorism group or a state-sponsored actor may be more interested in disruption than in financial gains that may choose against providing the recovery key regardless of payment.

Planning Considerations for Phase 3

For business continuity, the IT division of a health system must create contingencies for both the second and third scenarios. A backup copy on an entirely separate network or offline is the most meaningful [1]. However, regardless of the scenario, the perpetrator has no reason to help a victim organization clean its malware-afflicted computers. Additionally, no anti-malware software can definitively identify all affected machines, nor can one be sure that another cybercriminal group has not exploited the same weaknesses as the first. Just as an incomplete cancer treatment can recur and spread, a single malware copy can spread again within an incompletely cleaned IT infrastructure. For these reasons, regardless of whether the data itself is intact, recovered, or lost, a full recovery from ransomware attacks in all three scenarios necessitates a complete rebuild of the IT infrastructure using clean assets.

Phase 4—Reconciliation

While phases 1 to 3 are focused on ensuring operational continuity and providing safe patient care, eventually, the imaging data and reports will need to be reconciled with the patient's information in the EMR for continuity of patient care and to avoid loss of patient's medical data. The success of this phase will be heavily dependant on a well-organized phase 2 and 3. As a radiology department works with an analog workflow in the earlier phases, we will need to ensure that these records have the correct patient identifiers and order information and accession numbers to enable us for eventual reconciliation. The modality, technologists' information, communication information, and radiologist information will all need to be available for a smooth and correct reconciliation. The images (on CD/DVDs), order information, and reports will need to be stored securely in an organized manner to make them easily retrievable at a later phase. This reconciliation needs manual efforts as the images will need to be manually sent when the network is up and the radiology reports re-dictated in the system to interface with the EMR correctly.

Planning Considerations for Phase 4

Phase 4 differentiates an extended cybersecurity recovery effort from standard unplanned downtime. Data reconciliation and recovery may be necessary across multiple service lines after months of triggering downtime procedures. In our experience, a deliberate date-based approach has been most successful. In this approach, an imaging informatics professional begins by creating a workflow to process same-day examinations, either by direct ingestion using the new infrastructure or by offline reconciliation. Then, the reconciliation proceeds retrograde towards the date of the initial attack.

Previously analog reports also need to be digitized and reconciled with the appropriate patient and exam identifiers. While it is possible to perform this step by transcribing an otherwise complete hand-written report, in our experience, radiologists preferred to re-review examinations before signing off reports in the digital reporting system as the newly available EMR and prior exams can sometimes alter the diagnosis. Therefore, a dedicated report reconciliation and results communications workflow may be of value.

During the ongoing data reconciliation, the physician and technologist workflow can be complicated. For instance, examinations could be present on the ad hoc DICOM imaging archive system, on analog media, both, or neither (i.e., lost). For newly acquired examinations, the radiologist may need access to relevant prior studies that also may reside in one of many possible locations. Identifying the correct comparison examinations can be a challenge, as they may use either the reconciled (i.e., uptime) MRN and accession numbers or the corresponding downtime conventions.

Continuous Readiness Planning ("Phase 0")

Cybersecurity threats are unlikely to diminish. Instead, much of the management literature recommends including the recovery from cybersecurity threats to IT infrastructure as part of the standard business planning and cost. Therefore, readiness for a ransomware attack requires planning for an anticipated event and an ongoing effort to update and maintain these plans.

Therefore, the state of continuous readiness may be alternatively considered the "phase 0" of a ransomware attack in two ways. First, all IT infrastructure and end users should be regarded as vulnerable, their security risks manageable but not eliminable [4]. Second, the phase 0 mindset assumes that any day of normal operation could be followed by a

ransomware detonation the following day. Therefore, routine protocols may require modifications to meet the sudden need for the extended downtime. For instance, our breast imaging team now creates daily printouts of the next week's patient orders and schedules. Another imaging section began investigating daily backups of patient data in encrypted storage, either offline or on a separate network.

The following sections describe additional continuous readiness initiatives.

Cyberattack Response Task Force

At our institution, radiology and nuclear medicine created a cross-function Task Force to centralize the intradepartmental planning. Task Force members included leadership from physicians, nursing, technologists, front desk reception, administrators, operational leaders, quality and safety, imaging library, and informatics. The Task Force's mission is (a) to create the initial comprehensive and granular downtime plan in a unit-by-unit downtime manual. (b) After completing the initial recovery plan, the Task Force would be transitioned into a standing committee that periodically reviews and updates the reference documents and paper templates as part of the "phase 0" mindset, and (c) be part of the incident command.

Incident Command

We took the initial steps to create an imaging command center. The incident management system is highly regimented, and its details outside of this article's scope. However, it is worth noting that many organizations follow the Incident Command System (ICS) and National Incident Management System (NIMS) approach, provided via the Federal Emergency Management Agency (FEMA) [7]. ICS and NIMS take a standardized and modular approach with the command, operations, planning, logistics, administration, and finance. The construct is also designed for the interoperability of multiple incident management strategies to co-manage a situation, each of which may exist at differing severity levels. For instance, following a ransomware attack, our institution triggered an emergency response command center alongside an existing COVID-19 pandemic command center to manage the response to both incidences as they unfolded. While much of the work must be coordinated centrally, our experience showed that an imaging subsidiary could help coordinate the multitude of operational downstream impacts that can arise from a ransomware attack. FEMA offers online training courses for ICS and NIMS [7]. As the method is applicable to various emergency incidents, some caregivers within the radiology department have either already undergone training by preparing another emergency incident response through these resources.

Continuity of Operations Playbook

The COOP is designed to provide initial guidance for each operational unit to plan its step-by-step response plan and provide the executive leadership a birds-eye view of the recovery plan. Our organization created a recovery playbook template and distributed it to all of its departments for planning. Instead of listing the detailed step-by-step downtime procedure in the manual, the COOP focuses on a birds-eye view of the three sections' service lines.

The first section, Mission-Critical Services, lists the department's most essential activities, such as technical performance of stationary, portable, and on-vehicle imaging modalities, as well as interventional procedures. Each service is described using the informatics applications it requires and an outline of each phase's downtime planning instructions. For instance, while most modalities need RIS and PACS for image acquisition, "diagnostic reporting" is listed as a separate critical function because it further requires dictation software. Emphasis is placed on phase 1, which further subdivides into 0–2 h, 2–24 h, and 24–48 h, particularly for interventional procedural services where immediate patient safety requires special attention.

Whereas the Mission-Critical Services is introspective for the department, the COOP's second section, Interdepartmental Dependencies, is designed for cross-planning with and distribution to other departments. It lists the extended downtime contingencies with other organization departments such as outpatient clinics, inpatient units, emergency, and surgical units for intra- and peri-operative workflows. A phase-dependent response plan for operational continuity is recorded for each interdependency. This second section is most useful during interdepartmental planning, as the referring clinical units require an understanding of imaging workflow for their planning and vice versa.

The third section, Material and Resources, lists the items necessary to ensure downtime readiness. This section contains equipment requirements, such as pre-imaged offline backup computers and fax machines. It also has more nuanced material such as photocopier toners, CD/DVD media, paper templates, and office supplies like blank paper stacks and other material that would see a sudden rise in demand in extended, severe downtime. This material supply determines the number of days each operational unit's inventory can sustain an offline response.

Extended Downtime Manual

While the COOP provides a birds-eye view, the extended downtime manual is designed for the frontline caregiver and is specific for each unit, containing the pertinent information and protocols needed in case of a catastrophic ransomware attack. The need for an extended downtime manual stems

from the understanding that standard downtime procedures are insufficient for extensive ransomware attack recovery planning. For example, a typical downtime scenario is usually temporary (hours to a few days), and it is possible to use the standard communication tools like phone, emails, and intranet tools. Radiology accession numbers can still be generated, and temporary reports dictated, making reconciliation an effortful but uncomplicated task. Based on our experience and anticipated phase 4 needs outlined, these routine downtime processes are likely unavailable, insufficient, or both in a catastrophic ransomware attack. The extended downtime manual is designed to be printed, and the aim is to keep multiple copies available in critical areas and across different facilities across the system. A standard procedure would be created to keep the downtime manual refreshed and reprinted.

The Manual's Table of Contents (Table 1) is standardized, but it begins with a portion dedicated to the frontline unit where the Manual is deployed and is written by the unit's leader. For instance, the unit-specific content for a Manual deployed in outpatient CT may include phone numbers, printed references such as protocols, and detailed downtime procedures. The Manual for Imaging Informatics may include an initial section containing steps of communication,

Table 1 Table of contents for downtime manual

Unit-specific content	
1. Ransomware attack readiness checklist	
2. Unit-specific contact list	
3. Unit-specific reference material	
References	
1. Downtime operating procedures	a. Ordering b. Protocolling c. Image acquisition at modalities d. Image viewing and reporting e. Incident command center information
2. Key radiology phone/fax numbers	
3. Key organizational phone/fax numbers	
4. Summary of organizational downtime procedures	a. Nursing b. Pharmacy c. IT Division
Document templates	
1. Imaging report template	
2. Modality logs	
3. Imaging order requisition and instructions	
4. Additional standard forms	

a checklist of applications for availability assessment, an inventory of newly imaged backup hardware.

Additional sections are also included with references and templates developed and provided from central planning (Table 1).

Readiness Checklists

As with most highly subspecialized organizations, preparation requires a balance between centralized and localized planning. Therefore, we created a high-level readiness checklist for the radiologists in each subspeciality. This would focus more on adapting the departmental-level Downtime Manual to the section or facility's local needs. For instance, some unique workflows like intraoperative surgical foreign body assessment are handled by the emergency radiologists who will need to develop an analog workflow.

Routine radiologist workflows also need to be adapted for the offline and extended downtime. For instance, the only way to view images during phase 1 will be at the modality level, and all communications would need to be performed by phone or fax. Alternative coverage would require onsite radiologists coverage at all relevant hours. Additionally, radiologists might not have access to their work emails, and alternative modes of communication like a list of personal emails and phone numbers would need to be available for intradepartmental communication. Analog alternatives are also necessary for online resources such as an adrenal washout calculator or online bone age reference relevant to daily work. The checklist ensures that the reference information is available on paper or in a book format. Table 2 outlines our physician planning checklist, slightly edited for generalizability.

The outpatient reception, nursing, and technologist teams created a separate checklist specific to their functions.

Ordering and Reporting Templates

Replacing an entire IT-enabled workflow with paper analogs would require a more detailed discussion that addresses modality-level, departmental, and organizational nuances than possible in this article. Instead, this section highlights two templates, imaging order, and reporting.

Each hospital within our organization has its own downtime order requisition and formatting preferences. However, we have chosen to have a single standardized organization-wide imaging order requisition for standardization. Aside from contact information and signature from a licensed provider and patient identifiers, the requisition also includes a required "Communicate Results To" section. Additional fields include patient location, laboratory values, checkboxes for commonly ordered examinations, and a free-text section for unique protocol or procedures. This standardized

Table 2 Abbreviated readiness checklist for physician teams in radiology

Phase 0 (plan now—readiness)

☐ Plan for communication for a sudden outage within the section and with critical services
☐ Phone number and emails for the section
☐ Location to store downtime manual binder
☐ Assign a safe, locked location for documents containing patient information such as written reports.
☐ Engage enterprise collaborators on "special workflows"—for instance, stroke patients, intraoperative workflows, surgical foreign bodies
☐ Instructions for immediately needed processes like medication locker override
☐ Reference resources—such as book of protocols, textbooks (if needed)
☐ Alternative section schedule planning for at-modality interpretation
☐ Assess departmental interdependencies with other departments that you serve have a plan for communication with the departments

Phase 1—(first 48 h)

0–2 h
☐ Create protocol for immediate assessment to ensure the safety of current patients including diagnostic and procedural areas
☐ Identify a single downtime person to communicate with incident command
☐ Assess the extent of impact on workflow on diagnostic modalities
☐ Assess the extent of impact on workflow on diagnostic workstations
☐ Check phone lines and fax machines for functionality
☐ Identify the critical workflows that requires additional attention. E.g., Acute stroke
☐ Trigger paper-based ordering and results process for diagnostic examinations
☐ Trigger paper-based interventional procedure ordering and triage
☐ Prioritize immediate patient care demands. E.g. emergency, intensive care, urgent care, pre-operative, inpatient, outpatient
☐ Identify the examination types that require verbal results communication for every case

2–24 h
☐ Review items established during 0–2 h
☐ Determine the priority of future and pending outpatient orders. Which exams/if any must be cancelled/postponed so all remaining services can be properly staffed by physicians?
☐ Reassign staff as needed—staff might need to work off modalities till air-gapped independent systems are in place

24–48 h
☐ Review items established during 0–24 h
☐ Contact incident command for an updated status on operational impact
☐ Review plan for staffing changes and exam prioritization
☐ Identify imaging centers and locations no longer feasible for service, if any

Phase 2 (initial days to several weeks)

☐ Review phase 1 recovery plan
☐ Maintain contact with incident command for updated status and coordinate recovery of clinical operations
☐ Connect with IT for new digital assets such as clean offline computers
☐ Readjust physician task and shift modifications based on new workflow demands

Phase 3 (several weeks to months)

☐ Work with IT to have a backup copy on a separate network if possible and to plan for rebuilding infrastructure using clean assets

Phase 4 (several weeks to months)

☐ Paper-based workflow should have a systematic way to document patient and exam identifiers and record contrast and radiation dose (as needed)
☐ Transcribing the paper report to digital form would be needed to store this information in EMR
☐ Images stored on analog media should be correctly labeled to aid in eventual reconciliation with PACS and EMR

requisition is part of the Imaging Order Kit described under the section Organization-Level Coordination, which also includes instructions for caregivers not familiar with a paper-based ordering process.

Additionally, a survey of the existing downtime reporting templates reveals that most existing forms are optimized for convenience rather than data reconciliation. For instance, most templates are designed only for single-application downtime scenarios, affecting the dictation software only. Therefore, they include very brief sections of patient and exam identifiers as RIS and PACS availability are implicit. Many templates also label all downtime reports as "preliminary," which can confuse ordering providers. A preliminary report may be one that soon to be finalized at the end of the downtime procedure, or it can be one interpreted by a trainee radiologist. In an extended ransomware-related downtime, additional categories may be warranted.

Therefore, we developed a standardized extended downtime reporting template following the ACR Practice Parameter guideline for Communication of Diagnostic Imaging Findings [8]. We identified three report statuses: downtime preliminary, downtime signed, and final. A downtime signed report is the radiologist's best interpretation at the time of signing, which remains subject to change during phase 4 as

more data may become available. This approach allows the written reports to be organized and archived as they reach downtime signed status. The reporting template was jointly designed by imaging informatics professionals, technologists, and radiologists and supports the procedures detailed in their respective extended downtime manuals.

Organization-Level Coordination

Planning Considerations

While departmental planning is needed to define and develop processes, there are several organization-level considerations. One of the critical considerations is regarding patient identification. In imaging areas, a patient seeking care requires Medical Record Number (MRN) lookup, or a new patient may need an MRN assigned. This needs to be guided by the organization-level standard as unique patients identification needs to be homogenous across the different areas like radiology, labs, and clinical areas.

Another area that needs a coordinated effort is streamlining the ordering and reporting process with different clinical areas. Streamlining is especially important in situations that have a high impact on patient care like acute stroke protocol. Such protocols need to be identified. Each process needs to be defined: how the orders will be communicated, how the radiology report will be delivered, and how urgent findings will be communicated.

Some of the clinical workflows, like intraoperative workflows, are highly dependent on imaging, and the providers might not have access to images with the networks being unavailable. The images can either be made available on CDs, ensuring that the computers in the clinical areas have CD reading capability or setup alternative network for image viewing.

Other than these critical workflows, there are considerations on how we will continue to provide patient care in case of extended downtime. We developed an "imaging order kit" designed for inclusion in clinical departments' downtime manuals. The kit contains the following: (1) instructions on how to order studies in downtime, (2) numbers to call and fax order requisitions by location and modality, (3) a paper order requisition for photocopying, and (4) answers to referring providers' frequently asked questions including results communication, acquisition of patient images, intraoperative imaging, and others.

Tabletop Simulation

One of the more salient methods of integrating departmental planning into the rest of the healthcare organization is through a tabletop simulation [8]. Our experience in hospital-wide ransomware recovery tabletop exercises has been similar to that published in the literature, with multidisciplinary participation across all operational units [9]. During an organizational tabletop, the Task Force members' involvement alongside departmental executives can provide the much-needed insight into interdepartmental dependencies for the planning process. In our experience, the questions raised during the organizational tabletop serves as an excellent start to a departmental simulation.

For the departmental tabletop simulation, we used a similar framework published in the literature [9]. However, we focused on two ransomware-focused themes.

- Initial incident notification and communication—example scenario: a caregiver discovers a pop-up screen on the computer, describing that all files have been encrypted and that a "service fee" has been requested for the decryption key. ITD is notified of the messages. Shortly after, reports of an organization-wide network outage and inability to access RIS, PACS, and EMR began to surface. Example questions for discussion include the following:
  - Which patients are your responsibility at this time?
  - What are your immediate actions?
  - Which communication methods would remain available?
  - How would you communicate with your manager?
  - At what level does your service line connect with incident command?
- Operational recovery—example scenario: the outage sustains over the next 48 h. You have eliminated all immediate threats to patient safety. It is now clear that the ransomware has disabled much of the clinical resources you need for standard operations. Example questions for discussion include the following:
  - What are the extended downtime considerations for your unit?
  - Which other departments will be negatively impacted by operational interruptions in your service?
  - Which imaging services will you shut down?
  - Which imaging services will you sustain with at-modality, analog workflow?
  - Which imaging services will you prioritize towards an "enhanced" workflow using newly refreshed computers, local services, and ad hoc networking?

Conclusion

Ransomware attacks in healthcare organizations are increasing in prevalence. Disruptions in imaging workflow can have profound effects on the operations of the healthcare system. Proper business continuity and recovery planning for radiology should be central to any organization-level downtime planning. In sharing the planning framework, we hope to shed light on the operational complexity, the considerations, and the lessons learned that might serve as a starting point for the readers to begin these discussions in their own radiology practices.

Author Contributions P.C., R.B., and N.S.G. conceived of the presented idea. P.C. developed the concepts and frameworks. R.B. managed the implementation in the imaging institute. P.C. and N.S.G. supervised the work. All authors discussed the results and contributed to the final manuscript.

References

1. Cybersecurity & Infrastructure Security Agency, Federal Bureau of Investigation, Department of Health and Human Services. Ransomware activity targeting the healthcare and public health sector [Internet]. Cisa.gov; 2020 [cited 2020 Nov 27]. Available from: https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf
2. Cybersecurity & Infrastructure Security Agency. ICS Medical Advisories. 2020.
3. Kramer DB, Fu K. Cybersecurity Concerns and Medical Devices: Lessons From a Pacemaker Advisory. JAMA. 2017 Dec 5;318(21):2077–8.
4. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technol Health Care. 2017;25(1):1–10.
5. Cybersecurity & Infrastructure Security Agency. Ransomeware Guide. Cisa.gov; 2020.
6. Desjardins B, Mirsky Y, Ortiz MP, Glozman Z, Tarbox L, Horn R, et al. DICOM Images Have Been Hacked! Now What? AJR Am J Roentgenol. 2020;214(4):727–35.
7. Federal Emergency Management Institute. Emergency Management Institute - National Incident Management System (NIMS) [Internet]. Available from: https://training.fema.gov/nims/
8. Argaw ST, Bempong NE, Eshaya-Chauvin B, Flahault A. The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review. BMC Med Inform Decis Mak. 2019 Dec;19(1):10.
9. 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. 2020 Nov 24;