INFORMATION TECHNOLOGY FAILURES/CYBER INCIDENTS

Introduction

Cyber attacks on healthcare are increasingly common and increasingly disruptive. Intentional and non-malicious failures of both hardware and software can also result in downtime (i.e., the disruption of a facility or system's information technology [IT] services). In some cases, there is limited impact on a small number of systems. Other cases that affect the full active directory of programs or a major component such as the electronic health record (EHR) can result in severe impacts on patient care and business continuity. This chapter concentrates on the impact of system downtime rather than the IT aspects of the response and restoration of services.

Chapter Quick Links

There are a variety of ways in which systems can be compromised or fail. A few common examples include:

- **Physical compromise:** Fire, utilities/generator failures, hardware failure, and other physical damage can interrupt phone, internet, and other services and, depending on the system configuration, may also compromise multiple other systems.
- **Distributed Denial of Service (DDoS) attacks:** These attacks can overwhelm phone and internet systems, preventing the healthcare facility or system from communicating effectively. These attacks may also target community 911 and other mission critical systems.
- **Error in software/hardware transfers and updates:** Multiple software and hardware systems may fail during an installation or update process, even those not directly dependent on the software.
- **Ransomware:** These attacks involve deliberate accessing of systems with the intent of controlling software to demand money in return for restoration of access to data or platforms. Often, the "front door" for these activities is through external emails (e.g., phishing techniques). Systems that allow employees to use their own devices on the network may be particularly vulnerable.

Related Resources
Additional information is available on ASPR TRACIE's Healthcare Cybersecurity Resource Page, including Healthcare System Cybersecurity: Readiness & Response Considerations.

- **Internet of Things (IoT) manipulation:** Deliberate interference with the software/function of medical devices (e.g., intravenous pumps, electrocardiogram monitors).
- **Incidents with third party suppliers/vendors:** As illustrated during previous cyber incidents, attacks on third party suppliers can have cascading effects on hospitals and other healthcare facilities.
- **Other "infections:"** In some cases, viruses can cause system damage without an individual or group intent to seek monetary gain.

The impact from a cyber incident can be dramatic and prolonged. Major downtime incidents often have ripple effects for days to weeks due to the need to reconfigure computers, validate status for outside connected entities such as payors, and other restoration tasks. The facility or system will likely suffer financially from cancelled or reduced services, payment of ransom, fines, and replacement of hardware and software. Additionally, reputational harm can be done, particularly if protected health information is compromised. Most importantly for emergency management, patient harm can result from errors and delays due to compromised systems.

Healthcare has become extremely dependent on EHRs to not only document care, but for all ordering, results, quality data, and system monitoring. Though the EHR is often the principal software of concern, the EHR is almost always integrated with multiple notification, laboratory, radiology, pharmacy, ordering, billing, and other systems. A cyber incident can cause a domino effect of multiple systems experiencing concurrent downtime or lacking the inputs required to function. A growing number of hospital providers have never used a paper-based record system and have benefited from the built-in, digital order sets, cross checks, standardized dosing, and other features of the EHR. Similarly, providers may not have had experience calculating medication drip rates, which will be required if pre-programmed infusion pumps are disabled during a cyber incident.

Roles and Responsibilities

The role of emergency management is somewhat different in cyber incidents than most other emergencies in that there are two operational focus areas: service restoration and downtime operations. These must operate in sync with one another. In many cases, IT staff consider a cyber incident to be their responsibility and can take an insular approach to planning and responding to system interruptions. However, these incidents come with operational, financial, and even criminal considerations that make engagement of senior leadership and a strong incident command system (ICS) that unites the efforts of IT with clinical services and leadership imperative.

Emergency management is uniquely suited to bring together the partners during the planning process to ensure the following issues are addressed prior to an incident:

1. Systems mapping
2. Mitigation efforts
3. Preparedness efforts

4. Response planning
    a. ICS for downtime incident
    b. Recognition and initial actions
    c. Alerting
    d. Downtime procedures and activities
5. Recovery planning
6. Drills and exercises: Familiarizing staff with the downtime plans and forms helps prepare them for outages while also revealing weaknesses of the downtime documentation or plans.

Systems Mapping

One commonly overlooked activity that can be guided by emergency management is mapping the different IT/communications systems and documenting their intersection/inter-dependencies so that domino effect failures can be anticipated (and perhaps, if partitioning occurs early, prevented). Each system should also have an assigned downtime risk and a restoration priority so that life-safety systems are a focus for restoration efforts. IT staff often have a system map, but an interdisciplinary approach to understanding the relationships between the systems and their relative priorities (specific to patient safety and ability to create safe workarounds) helps foster joint understanding between IT and clinical operations staff.

The systems map can then serve as an outline during response, helping hospital leadership and IT staff understand implications of the systems that are down and prioritize system restoration based both on the impact and the time and effort to restore functionality. The systems map should also consider how, if usual integration is not possible, each system will operate independently (e.g., how are laboratory results accessed via an alternate interface if the EHR remains down?)

Mitigation

Mitigation of a downtime incident is a focus area for all healthcare IT and this section provides just a few examples. Prevention of phishing attacks, keeping software updated, practicing email hygiene, preventing use of programs that can allow malicious code into the system, and use of firewalls, protective software, and redundant and fail-over systems all contribute to reducing the risk of downtime.

From the Field
Some hospitals use external consultants to probe their systems for vulnerabilities (e.g., “white hat” hacking) or deliberately create hoax emails to test how many employees follow links or provide information. This can help identify systems and educational issues that may reduce future risk from a hostile entity.

Policies should be in place to encourage rapid reporting of system problems (e.g., systems exhibiting abnormal behavior). Authority should be granted to IT personnel to shut down or isolate systems as soon as a potential

problem is recognized to try to limit spread and damage, even if this means taking major systems offline while the problem is investigated.
Note that some mitigation activities that restrict the use of certain software (e.g., ability to access external email or share documents) to prevent system infection can limit the contingency options for communication and coordination when systems go down.

Preparedness

Many hospitals do not adequately prepare for downtime incidents. This section briefly summarizes key considerations. Similar to other hazards that require specific response actions (decontamination, mass casualty), hospital emergency management may wish to create a playbook for major downtime incidents that includes elements from this chapter as well as specific issues and strategies identified through facility assessment and exercises. This ensures a proactive approach during the first several hours of the incident by the incident command team that hopefully can provide a foundation for the remainder of the response.

Many hospitals and healthcare systems maintain laptop computers that are disk imaged to support clinical operations but are deliberately kept off the network and have software upgrades that lag those in real time, ensuring that at least some computers will remain unaffected. Additionally, having the ability to cable-connect to printers on each unit may be invaluable.

Most EHRs mirror routinely so that in disaster recovery mode it is possible to look back at the status of departments and patients at the time the system went down. Employees should know how to access this system immediately when a downtime occurs. The value of the information decreases as time goes on. There should be a threshold point at which key information should be transcribed to paper by the care team (e.g., six hours or more of expected downtime) so that ongoing changes can be captured along with prior information.

Some hospitals run paper snapshots each day. This may be unit-based or hospital-based and the depth of data varies depending on facility preference. Other facilities run paper-based summaries prior to software upgrades, during weather warnings, or based on other events. Unfortunately, most cyber incidents occur without warning.

From the Field
When a hospital experienced cascading failures of most major systems due to a fire, a patient list that was printed that morning showing all admitted patients and their units was critical to successful patient evacuation and tracking.

Redundant internet providers (e.g., satellite-based, cellular-based with hotspots) and communications equipment (e.g., downtime cellular phones, handheld radios) can help ensure continuity. Training individuals in key positions in how and when to use this equipment is also important.

Policies also should include downtime processes for documentation, ordering, and results communication. Downtime processes for accounts receivable and payable and for ordering from external suppliers should be included.

Note that some of these policies will be crosscutting (e.g., what to do when phones are down) but many will be specific to the area (e.g., laboratory management of equipment downtime, reporting system interface down). For example, many laboratory analyzers require logging in and are tied to the IT system active directory. Contingency plans must be in place for any device that is network-connected (e.g., develop plans to use handheld or other analyzers for emergency lab values or externally source laboratory services).

Paper forms should be available and optimized to the area. For example, templated forms should be customized for outpatient clinics, emergency departments, surgical services, and different levels of inpatient care, and pre-printed order sheets should be available to guide providers who are accustomed to computer templates. This requires significant work, and it may be beneficial when a new order set (e.g., diabetic ketoacidosis) is produced in the EHR for the author to develop a concise downtime form at the same time. Screenshots of the EHR ordering pages/sets are *not* sufficient.

From the Field
During a prolonged downtime at an academic medical center, leadership recognized the first day that the volume of paper required multiple staff to collect, sort, index, and box records. These records were secured in conference and other rooms.

Copies of all paper forms should be available not only on the network but also on hard drives and USB drives that are stored separately. Maintaining additional printers, including thermal printers for labels and wristbands, and adequate supplies of paper and toner onsite until resupply is provided is also suggested. Adequate hard charts (e.g., tabbed binders) and paper forms for the first 48 hours of facility operations should be immediately available on the units and in storage (e.g., in pharmacy, laboratory, radiology, nursing administration). Downtime generates large quantities of paper, much of which contains protected health information. Sets of banker boxes should be kept available and locked space in administrative areas identified where records will be kept until they can be digitized during recovery.

Staff must have exposure to downtime procedures and forms on a routine basis, so they know when and how to initiate downtime procedures. Job aids and other prompts on the clinical units can support a successful transition. Drills and exercises should be conducted to increase familiarity and evaluate the performance of the downtime materials and policies for improvement. There may be a role for retired clerks, nurses, and providers to assist with developing downtime procedures and serving as potential surge staff in the event of a downtime incident as they are familiar with paper-based systems and can assist with charting, coaching, organizing, and filing.

Drill and Exercise Considerations

The Greater New York Hospital Association and the Cybersecurity and Infrastructure Security Agency developed exercise scenarios across the following categories that may help other hospitals consider elements to include in their own drills and exercises:

- **Policy** – Focuses on executive decisions, communications, ransom decisions, interface with legal/law enforcement.
- **Operations** – Focuses on patient care delivery, particularly care transitions (e.g., movement of a patient from the ED to the operating room to inpatient room) that involve tracking and information exchange.
- **Frontline Staff** – Focuses on immediate actions by staff when systems behave abnormally or crash and near-term patient monitoring (e.g., patients who are no longer on telemetry) and documentation needs.

Response

Once IT personnel recognize an incident, there should be a policy for alerting staff to the systems that are down, actions to be taken, and expected duration (if known). This should include instructions about whether to initiate downtime procedures. IT management should expect ICS to be activated and be prepared to brief leadership on the impact, origin (if known), current status, and actions taken.

Cyber attacks tend to result in relatively closed-door communications and decision-making between IT personnel and hospital leadership. This should be expected and planned for. Some information will be highly sensitive (e.g., involving ransom, criminal investigations) but IT staff and hospital leadership should provide the rest of the incident command team information that can inform ongoing downtime and clinical operations. The executives and IT leads often involved in these decisions usually are also needed by incident command to help troubleshoot, provide whatever information is available about restoration, and support adaptive strategies based on facility needs.

Internal and external communications need to be vetted with leadership (including legal counsel) and public relations. The Public Information Officer (PIO) should ensure staff, inpatients, outpatients, other facilities in the area, and the public's needs are all considered and develop talking points - updated as often as possible - to meet those needs.

The Operations Section should be divided into two branches, one for IT Operations and one for Clinical Operations. The Operations Section Chief can then help bridge clinical and IT information and issues and inform the Incident Commander of key problems and resource needs. Note that during prolonged incidents, staff should incorporate improvements to ensure that forms, processes, and policy are modified to streamline the ongoing response and inform future responses.

The Planning Section should establish operational periods and, if the downtime is likely to continue, determine logistics needs and develop operational recommendations (e.g., cancelling or restricting outpatient visits) for the next shift/day. The Planning Section should work closely with the Operations Section to anticipate policy and resource needs as the downtime continues.

The Planning Section should anticipate that all areas will need additional staff support. Runners, scribes, and additional clinical staff (particularly nurses) will be needed to maintain operations as workflows will be severely interrupted. During a prolonged incident, contracted nursing staff may be needed. The mental and physical stress on staff may be severe. There is a high potential during a protracted incident for absenteeism to increase and attracting external staff on contract will be difficult. Providing behavioral health and physical staff support throughout the incident will be critical to preventing/managing fatigue, minimizing errors, and promoting overall resilience. Multiple options for workforce supplementation should be considered (e.g., students/trainees, Medical Reserve Corps, retirees, volunteers). In many roles, specific medical knowledge is not needed to be helpful.

The Planning Section will likely need to lead several multi-disciplinary teams across business, clinical care, and hospital operations to determine what contingency strategies need to be invoked based on key areas of impact and risk. In most cases, this will occur through a problem-focused, cross-functional approach and may include such issues as:

- **Archiving processes:** How will downtime materials be indexed and that information integrated back into the medical record?
- **Purchasing and payroll:** How are purchases made and contracts executed? How are supplies monitored? How will employees get paid?
- **Billing:** What is the process for submitting claims and what are the thresholds for payors to receive electronic information from the system once it is restored?
- **Scheduling:** How are outpatient visits scheduled? How are the staff scheduled if these systems are affected?
- **Results reporting:** How are critical and routine results reported to clinical staff in a timely way? Can temporary communications systems be instituted to ensure rapid reporting and loop closure?
- **Clinical orders:** How is loop closure maintained? What improvements can be made in the ordering process to improve efficiency and safety?
- **Clinical services prioritization:** What type and volume of services can be offered based on the impact? What options exist for prioritizing care?
- **Staff communications:** If notification and/or email systems are down, what contingencies can be created?

The Planning Section is also responsible for creating situation reports and managing documentation. The Documentation Unit Leader will need to work closely with medical records, registration, and other departments to ensure that downtime work is saved with methods and indexing that enable continued access if needed. Dedicated personnel will be needed to index, label, and file paper documents. If the downtime is prolonged, a chart audit process will be needed to ensure charting completion for a patient encounter. A decision should be made early about whether to scan or abstract the paper documents contemporaneously. Paper and scanned materials should be available to the care teams in a Health Insurance Portability and Accountability Act (HIPAA)-compliant manner for reference.

The Planning and Operations Sections should work closely to determine what systems *are* working and can be leveraged to improve documentation and messaging. For example, phone-based apps can be used for drug calculations and other references as well as for voice-to-text dictation that may be able to be integrated into charting. Messaging apps may be valuable in communicating critical information and results (with appropriate attention to respecting protected health information as common messaging platforms are not HIPAA-compliant).

Regional coordination is an important consideration. When a hospital is experiencing a significant downtime, it often diverts ambulances to other hospitals or curtails services, resulting in additional volumes for other facilities in the area. If multiple hospitals are part of the same system and all experience an incident, this can have profound implications for care. Even if certain information cannot be shared, situational awareness of impact should be maintained within the region and efforts made to ensure safe continued operations by balancing risk and patient loads within the area. Healthcare coalitions can be a valuable convenor and source of coordination and information.

Recovery

Recovery from an IT downtime incident begins during the response. Incident command must make decisions with IT about a service restoration plan that often will be staged. Communication with staff about timelines, managing expectations, and instructions on resetting equipment, passwords, and other tasks will be important for a smooth transition.

Incident command should *not* be stood down when the system comes back up. Problems can occur even after a short-term interruption has been addressed. In a longer incident, the incident command structure will continue to be needed to oversee the archiving process, re-integration with external systems, and other tasks.

The priority will be to get clinical systems up and running as soon as possible. Independent testing of the systems will usually be necessary before connections can be made to transfer information for purchasing and billing purposes to assure external entities that there is no residual risk. This can take days to weeks.

Processes for organizing documentation, ensuring chart completion, and determining billing should be established early in the response phase to facilitate recovery. Information will need to be transferred from paper into electronic format; this may involve a combination of manual entry, scanning, or dictation. Ideally, decisions about what will be entered into the chart and by what method should be made prior to an incident, but certainly early in the incident so the process can start as soon as systems come back up. The volume of information generated can result in weeks to months of work to restore, and incident command will have to continue to devote significant resources to archiving. After conversion, paper records will need to be destroyed in a HIPAA-compliant manner.

Staff recovery will take time. Residual frustration and anxiety are likely. Continued staff support and engagement will be needed. Staff should be empowered through the after-action process to provide suggestions for improving future responses.

As with any incident, hospital emergency management should oversee a comprehensive after-action review that identifies areas of success and areas for improvement. A corrective action plan should be generated to guide changes to policy and process for future incidents.

Depending on the situation, criminal or civil legal issues may take months or years to resolve. Evidence collection, depositions, and other tasks may consume significant resources. Liaisons with multiple external agencies may continue for weeks to months. Other legal and regulatory issues may require dedicated resources.

In summary, the recovery process is long and complicated. Incident command may be needed for a protracted period although the activation can usually be downsized after service restoration.

Conclusion

Few incidents involve as many unknowns as a cyber incident, and the duration and impact on staff and patient safety of a major downtime incident is likely to be significant. Almost every operational area needs to undertake specific planning efforts, adding to the complexity for the emergency manager. Most hospitals do not have adequate plans, documents, and policies in place to effectively operate safely with major systems down. Thus, IT/cyber incidents should be a focus of planning for emergency managers. Starting an incident with clear policies, processes, and a playbook of initial actions can make a major difference in the outcome. Intra-event learning and developing adaptive processes can also offer significant benefit during a prolonged incident and should be an incident command focus.

Acknowledgements

ASPR TRACIE thanks the author of this chapter, **John Hick**, MD, Hennepin Healthcare and Senior Editor, ASPR TRACIE, and the following subject matter experts who comprehensively reviewed it (listed alphabetically): **Scott Gee**, Deputy Director for Cybersecurity and Risk, American Hospital Association and **Nicole Ziogas**, MPH, Senior Project Manager, Emergency Preparedness, Greater New York Hospital Association.