Academic Medical Center | Patient Safety Organization

a component entity of Risk Management Foundation

Patient Safety Alert

Cybersecurity and Recovery

Issue 32 | 2023

Introduction

In 2016, the AMC PSO assembled a task force of subject matter experts (SMEs) to share their experiences in preventing, responding to, and recovering from electronic health record (EHR) downtime events. That group focused on preparing for downtime; activating a response to it; communicating during it; implementing paper-based EHR documentation and ordering; monitoring patient safety risks during downtime, and the steps to take toward recovery. Those SMEs created a guidance document (www.rmf.harvard.edu/ehrdowntime) summarizing their recommendations.

In 2022, AMC PSO members identified new threats and reviewed case studies of events within health care systems that had resulted in a loss of function of integrated IT systems including, but not limited to, the EHR. These threats now include ransomware, denial of service, and other cybersecurity attacks that present a daily threat to health care systems. Cybersecurity attacks topped the ECRI list of the *Top 10 Health Technology Hazards for 2022*. With this background, the AMC PSO once again gathered SMEs to review our previous work and add recommendations to our original guidance based on the most common threats and events experienced today in global health care systems.

The 2022 group supported the recommendations from 2016 as still valid and suggested additional recommendations for organizations to consider as they contend with evolving risks. These included updated specificity on how best to prepare, activating a hospital incident command, communication strategies, recovery planning, and the patient safety implications of events related to cybersecurity attacks.

Preparing for a Cybersecurity Event

Conduct a Business Impact Analysis (BIA) to identify key systems, processes, and integrations along with viable alternatives for the high-priority functions. Conduct these analyses with each business unit, keeping in mind that there are potentially thousands of applications and integration points. Consider the most critically important ones first. In addition, look at SAAS-based systems (e.g., payroll systems) when conducting the BIA. Finally, scrutinize legacy systems where software support no longer exists. If there are old versions of software in use, they may pose risk in the face of a complicated recovery process. Use a rational, patient safety-centric approach for prioritizing how to best conduct the BIA process.

A Security Incident Response Plan should include specific playbooks on how to manage and respond to a large-scale security event such as a ransomware attack. These playbooks will be part of your overall Disaster Recovery plan that identifies the processes and procedures for resuming normal operations after such an event. Both plans should be tested between the IT and clinical staff at least annually, preferably quarterly.

Conduct tabletop exercises that engage Senior Leadership, including clinical and operational leaders, IT, Communications, Legal, and Government Relations teams. In cybersecurity events, these groups will be highly active in the HICS structure and crucial to successful response and recovery. Create specific roles for the legal, communications, and government relations teams. An added benefit of including senior leadership is raised awareness of the finances required to maintain strong Cybersecurity and Emergency Management departments. Consider including your cyber insurer and a representative from the FBI (or local state agency) in the drill.

In addition to these drills, annual training for all employees on the basics of downtime response is suggested. Remember, as these events may go on for days or even weeks, it is important to plan for the backup roles needed in your HICS chart to allow for rest by the key leads.

The SMEs convened by the AMC PSO remain concerned about the siloed activity among departments with IT and the health care system's operations teams. Full coordination and cooperation when planning for these service disruptions remain a challenge. The inclusion of IT and healthcare systems operations teams in drills is essential for building more collaborative relationships and modeling and testing what will work best in an actual event.

Initial and full Downtime Assessment and Response Teams (DART/iDART) are typically identified within the Disaster Recovery policies and associated processes. A common term used is Maximum Tolerable Downtime (MTD)—the maximum amount of time a core system/service can be unavailable before enacting Disaster Recovery processes. A defined and published MTD is critical to ensure the team knows when to begin recovery processes.

Ensure that downtime carts are maintained and that there are just-in-time instructions attached to the carts to supplement any training that might happen

Definitions

Ransomware

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption.

Denial of Service

When legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious actor.

Disaster Recovery

An organization's method of regaining access and functionality to its IT infrastructure after events like a natural disaster, cyber-attack, or other business interruption.

DART or **iDART**

Acronym of disaster assistance response team or initial disaster assistance response team.

MTD

Maximum tolerable downtime is the amount of time mission/business processes can be disrupted without significant harm to the organization's mission.

SAAS

Software **A**s **A** **S**ervice is a method of software delivery that is accessed online via a subscription rather than bought and installed on individual computers.

HICS

Hospital Incident Command System based on principles of Incident Command System, which help health care organizations improve emergency management planning, response, and recovery capabilities on hire or annually. Also: consider the fact that the pandemic has resulted in workforce shifts, including increased use of temporary employees so a just-in-time education is warranted. Consider alternate communication technology strategies if all e-mail communication is unavailable.

Drills and plans should also include focused consideration on critical data recovery: prioritizing how you would recreate data/patient records if unable to ultimately recover lost data. How would you prioritize which clinical care items are essential? Would you first recreate medication lists, laboratory data, or other treatment regimen data? The ability to proactively prioritize based on tabletop simulations can serve to reduce the time for decision-making during an actual event.

A free resource recommended was *Get Your R Score* (www.getrscore.org/) This is a tool to assess your organization's data recovery readiness in the event of a ransomware attack.

Activating Response and Downtime Procedures

In cybersecurity events, initially assume that full compromise of systems has occurred.

Activate alternate communication technology. Ideally, stacked solutions for communication will have been clearly described in the planning process.

A key to success is a strong emergency operations and disaster recovery plan, as well as operational leaders adequately prepared for downtime decisions. Clear communication plans, with associated roles and responsibilities, should be outlined in the emergency operations plan.

Another important factor is a strong HICS structure that ensures everyone is following the documented and tested plan. This is especially important in complex systems where clinicians may still attempt to access systems that have not yet been fully approved as operational, contributing to confusion about which systems are up and running vs. compromised. One suggestion is to have two teams: one responsible for ensuring systems have been scrubbed of all malicious Software (Malware) prior to use and a second to monitor the operations as the systems come back into use. This will assist with collaboration between the health systems operations functions and the IT teams.

Communication Considerations

The HICS communications and government relations sections become particularly important in these events due to the need for coordination with federal and state agencies and with the media. Establish and test your standardized and well-publicized alternate communication system, for internal and external communications.

During the downtime event, the communications team should articulate and communicate timelines (even if only range approximations) and next steps. Recognize that, in some of these events when there is the involvement of external agencies and not all information may be shared, updating the staff remains essential.

Disaster Recovery

Disaster Recovery and Incident Response plans should consider storing critical electronic recovery documentation and system credentials in two locations: both a non-integrated cloud-based system and an external portable storage media device. (The portable media device should be password protected and encrypted.) Storing this critical information in a system on-premises may result in the inability to retrieve it during a cyber event. These are decisions to be made as part of building out your Disaster Recovery plan. Tabletop exercises and real-time testing can identify gaps in backup plans. Processes for procurement should be in place, as part of the Disaster Recovery plan. Processes and playbooks should be part of the Disaster Recovery and Incident Response Plans and should contain prioritization of assets for restoration after the core infrastructure is restored.

Remember that for both simulations and real-world events, a lessons-learned debrief is always the ultimate step in an Incident Response Plan

Focused consideration on data recovery includes: prioritizing how you would recreate data/patient records if you are unable to recover lost data. How would you prioritize? Would you first recreate medication lists, the ADT system, Laboratory data, or other treatment regimen data? The ability to proactively prioritize based on tabletop simulations can save time during an actual event.

Regional Cooperation

One of the considerations discussed by the SMEs in our AMC PSO discussion was related to the potential for regional collaborations across institutions to bolster support for an attacked organization when a long recovery period is anticipated. At present, many institutions will lack sufficient IT resources to sustain the amount of intensive, long-term work over the course of months to recover from a sophisticated attack. In addition, clinicians may not be able to operate essential devices to manage critical care. Planning ahead for the potential need for regional cooperation with joint tabletop drills may be something to consider for future planning.

TASK FORCE MEMBERS

Paul Biddinger
Mass General Brigham

Tricia Bourie
Beth Israel Lahey Health – Beth Israel Deaconess Medical Center

Jeannette Currie
Beth Israel Lahey Health

Mary Devine
Boston Children's Hospital

Ann Marie Dwyer
Massachusetts General Hospital

Heather Fowles
Mass General Brigham

Jennifer Hendrickson
Mass General Brigham

Melissa Lantry
Massachusetts General Hospital

Jonathan Morley
Tufts Medicine

Heather Nelson
Boston Children's Hospital

Rajesh Patel
Beth Israel Lahey Health

Paula Wolski
Brigham Women's Faulkner Hospital

Michael Wiker
Wentwork Douglas Hospital

Catherine Schroeder
Mass General Brigham

CRICO MEDICAL WRITERS

Yvonne Cheung, MD
Associate Medical Director, AMC PSO

Patricia Folcarelli, PhD, MA, RN
Vice President, Patient Safety

Jennifer Clair MacCready, DNP
Senior Program Director, AMC PSO

John Fanara
CISO and Director of Information Technology

CRICO PROJECT STAFF

Alison Anderson
Principal Art Designer

Carol Ann Garcia
Senior Program Administrator

Wallinda Hutson
Senior Information Resources Librarian

For permissions and secure methods of communication to the AMC PSO, please contact: amcpso@rmf.harvard.edu, 617.450.5586