Mass General Brigham

Downtime Readiness in Healthcare Operations

Jennifer Hendrickson, Director of Emergency Preparedness and Continuity, Mass General Brigham

April, 2024

Agenda

Introduction

Learning Objectives

Overview of the problem

Multi-disciplinary approach and solution

Accounting for cascading impacts and third parties

Example tools and resources

About Mass General Brigham

Mass General Brigham is an integrated academic health care system, uniting great minds to solve the hardest problems in medicine for our communities and the world. Mass General Brigham connects a full continuum of care across a system of academic medical centers, community and specialty hospitals, a health insurance plan, physician networks, community health centers, home care, and long-term care services. Mass General Brigham is a nonprofit organization committed to patient care, research, teaching, and service to the community.

In addition, Mass General Brigham is one of the nation's leading biomedical research organizations with several Harvard Medical School teaching hospitals.

Patient care

From routine care to the most complex cases, we offer comprehensive, full-circle clinical care to our patients, starting and ending at home.

Research and discovery

Because we are built on a legacy of medical discovery, our researchers push the boundaries of knowledge and advance medicine in new and innovative ways.

Teaching

We have over 100 accredited physician residency and fellowship programs, and over 2,000 trainees preparing to be the healers of tomorrow.

Community

We have five licensed and 15 affiliated community health centers. We have diverse community partnerships to support our local residents.

Mass General Brigham at-a-glance

$16 Billion
Total Operating Revenue

$2+ Billion
Over $2.2 Billion in research activity with more than $1 Billion in direct DHHS funding

Mass General Brigham System

12	Acute and Specialty Hospitals
5	Harvard-affiliated Teaching Hospitals
28	Rehabilitation Locations
4	Ambulatory Surgery Centers
22	Urgent Care Centers
5	Community Health Centers

Largest Private Employer in Massachusetts

~7,000
Physicians & Fellows

82,000
Employees

2.5 Million
Unique Patients

FY22 summary data

MGB Department of Emergency Preparedness and Continuity

- MGB has benefited from strong collaboration on emergency preparedness efforts across the system for many years. However, complex responses to Ebola, COVID and other events helped identify opportunities to better use personnel and resources to improve system coordination of emergency preparedness and business continuity activities.

- The DEPC was created to address variation in readiness programs across MGB, to identify and mitigate any gaps, to facilitate sharing of expertise and staff, reduce duplication of efforts, and to improve overall program quality.

- Benefits of a single system-wide DEPC:
  - Synchronize and optimize emergency operations at entities across system
  - Lead cross-functional initiatives that improve readiness
  - Harmonize strategic efforts that address risk
  - Create sustainability plans and infrastructure for business continuity
  - Improve support to cross-cover staff and MGB entities

MGB Department of Emergency Preparedness and Continuity

- Ensuring vulnerable populations and equity are at the center of our planning and response
- Enhanced enterprise emergency planning, including continuity planning, to ensure a coordinated and integrated approach to supporting all of our MGB Community
- Working across departments with key stakeholders to study and take action to make our facilities and infrastructure more resilient
  - Partnering with facilities, engineering, finance, insurance, quality/safety, among others.
- Increasing our advocacy efforts to local, regional, state and federal levels because we cannot become resilient alone
  - We rely on community infrastructure and our patients rely on common infrastructure
- Developing better measures and metrics to chart our progress
  - Improving risk analysis and associated metrics to better measure risk reduction and benefits to our communities

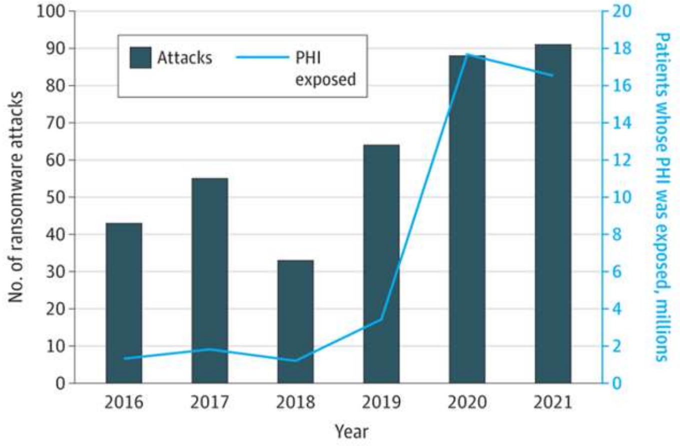
Overview of the Problem and Learning Objectives

Learning Objectives

- Integrate downtime readiness into all-hazards emergency operations, continuity planning and response structures for healthcare organizations and systems.
- Develop a multi-disciplinary downtime readiness program with an associated governance structure to promote a coordinated and unified approach to planning, incident response and recovery operations.
- Identify key partners within healthcare organizations to participate in downtime readiness planning and response.
- Provide example tools and structures to support healthcare organization/system downtime readiness (i.e., downtime toolkits, training models).
- Understand the cascading impacts and plans needed for cyber attacks (or prolonged downtimes) on hospitals within your coalition, including communication challenges, and third party vendor management.

Overview and Scale of the Problem

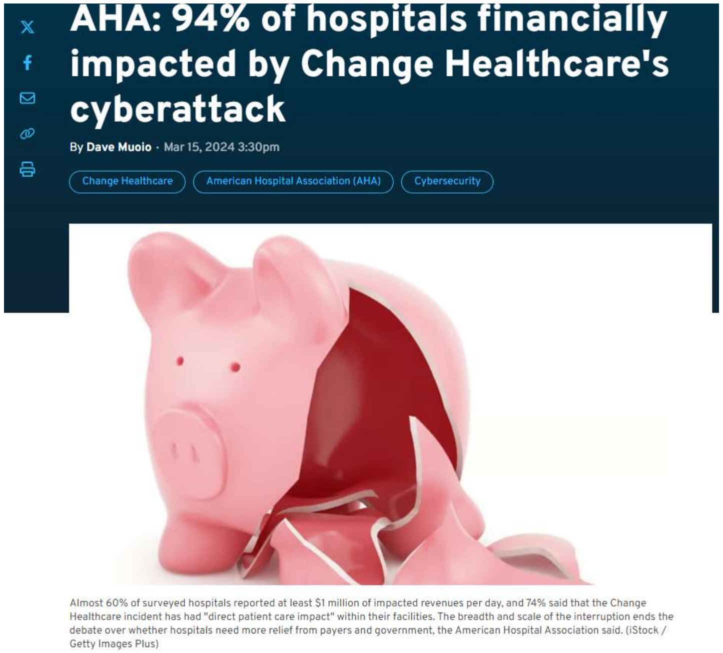
- Healthcare operations rely heavily on digital applications and systems. The integration of these digital systems with critical operations is continuing to grow.
- Unplanned disruptions to our critical applications can arise from a number of different factors including vendor disruptions, maintenance issues, cyberthreats and more.
  - ***Downtime incidents are a significant threat to our operations that have critical impacts on delivering safe patient care in a timely and effective manner.***
- Of special note, the healthcare industry in the US has experienced a significant increase in the number of intentional digital incidents, including ransomware and cyber-attacks, that can lead to extended downtimes.
- Cyber incidents and more broadly disruptions to our digital systems and to third party vendors are routinely ranked as top risks on Hazard Vulnerability Assessments.



Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021, JAMA Health Forum. 2022;3(12):e224873. doi:10.1001/jamahealthforum.2022.4873

Data shows that many healthcare downtimes can last **for 4-6 or more weeks**.

Recent Notable Events



AHA: 94% of hospitals financially impacted by Change Healthcare's cyberattack

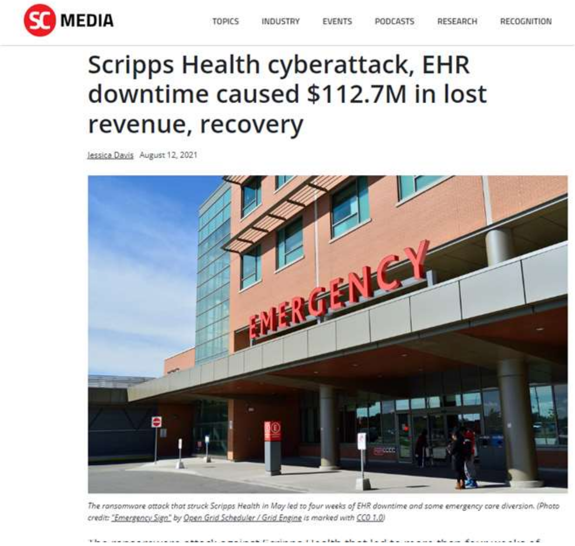
By Dave Muoio · Mar 15, 2024 3:30pm

Change Healthcare | American Hospital Association (AHA) | Cybersecurity

Almost 60% of surveyed hospitals reported at least $1 million of impacted revenues per day, and 74% said that the Change Healthcare incident has had "direct patient care impact" within their facilities. The breadth and scale of the interruption ends the debate over whether hospitals need more relief from payers and government, the American Hospital Association said. (iStock / Getty Images Plus)

HEALTH IT SECURITY
xtelligent HEALTHCARE MEDIA

UVM Health Brings EHR Back Online, One Month After Ransomware Attack



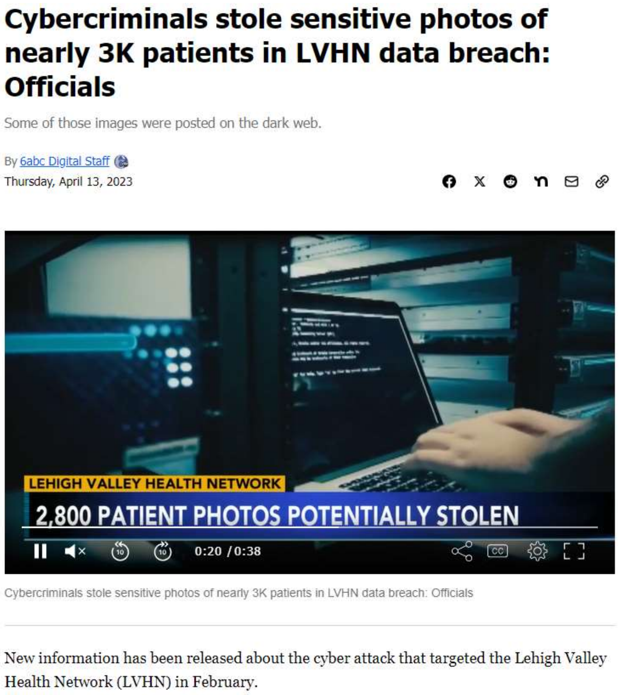
SC MEDIA

Scripps Health cyberattack, EHR downtime caused $112.7M in lost revenue, recovery

Jessica Davis August 12, 2021

The ransomware attack that struck Scripps Health in May led to four weeks of EHR downtime and some emergency care diversion. (Photo credit: "Emergency Sign" by Open Grid Scheduler / Grid Engine is marked with CC0 1.0)

The ransomware attack against Scripps Health that led to more than four weeks of



Cybercriminals stole sensitive photos of nearly 3K patients in LVHN data breach: Officials

Some of those images were posted on the dark web.

By 6abc Digital Staff
Thursday, April 13, 2023

LEHIGH VALLEY HEALTH NETWORK
2,800 PATIENT PHOTOS POTENTIALLY STOLEN
0:20 / 0:38

Cybercriminals stole sensitive photos of nearly 3K patients in LVHN data breach: Officials

New information has been released about the cyber attack that targeted the Lehigh Valley Health Network (LVHN) in February.

One Approach to Downtime Readiness

All Hazards Integration

Given the heightened threat of cyber events and the high rank of cyber incidents/hazards in our risk assessments, MGB integrates cyber and downtime preparedness into our all-hazards planning and approach.

- Emergency Preparedness works closely with the MGB CISO and the MGB Digital Teams on threats to our infrastructure from malware, ransomware, etc.
- Enhanced coordination and collaboration is critical and ensures efficient and effective use of resources, removing silos.

The MGB Department of Emergency Preparedness and Continuity facilitates this work and collaboration among a multidisciplinary group of stakeholders.

- EP structured and integrated into healthcare organizations to:
  - Prioritize diverse response actions and support a coordinated response.
  - Increasingly relied upon to respond to complex organizational challenges that continue to arise.

MGB Downtime Readiness
Committee Framework

	Entity	Enterprise	Executive
Meeting Frequency	Monthly	Bimonthly	Triennially
Committee Chair(s)	COO Designated	Emergency Preparedness, Digital and Operations	Emergency Preparedness and Digital
Primary Membership	• Entity Digital • Emergency Preparedness • Clinical Operations • Quality and Safety • Nursing Informatics • Chief Medical Information Officer • Others as deemed appropriate by facility leadership	• Representative from each Entity Downtime Committee • Digital, InfoSec, CMIO, and EHR representatives • Emergency Preparedness • Office of the Chief Quality Officer • Telecom • Communications • Health Information Management • Capacity or Enterprise Asset Management	• Deputy Chief Operating Officer • Chief Preparedness & Continuity Officer • Chief Information & Digital Officer • Chief Information Officer • Chief Information Security Officer • Chief Quality Officer • VP for Compliance • Chief Academic Officer (Research)
Purpose	• Identify frontline operational issues and needs • Review and implement system protocols, procedures • Facilitate local trainings and exercises • Facilitate local downtime equipment checks • Plan for scheduled downtime events • Conduct local follow up after incidents and events	• Discuss readiness and response standards • Collect and respond to frontline downtime needs and issues affecting the system • Support the development of toolkits, resources, exercises • Facilitate continuous improvement processes for the system • Coordinate mitigation efforts • Assist with prioritization of the enterprise downtime initiatives	• Ensure accountability for downtime readiness • Approve major system downtime policy and priorities • Approve initiatives requiring major funding or that may cause disruption to operations (such as downtime training and exercise programs)

Downtime Readiness Governance Structure

Goals

Identify, monitor, and understand downtime risks

- Conduct continuous assessment and review of downtime threats and hazards. Give these risks context within MGB, while understanding their projected operational impacts.
- Monitor continuously, address new risks and understand their impact on the system

Promote unity of effort

- Implement a coordinated unified approach to planning, incident response, and recovery.
- Provide a foundation to ensure consistent and complementary response and recovery operations during a downtime incident.

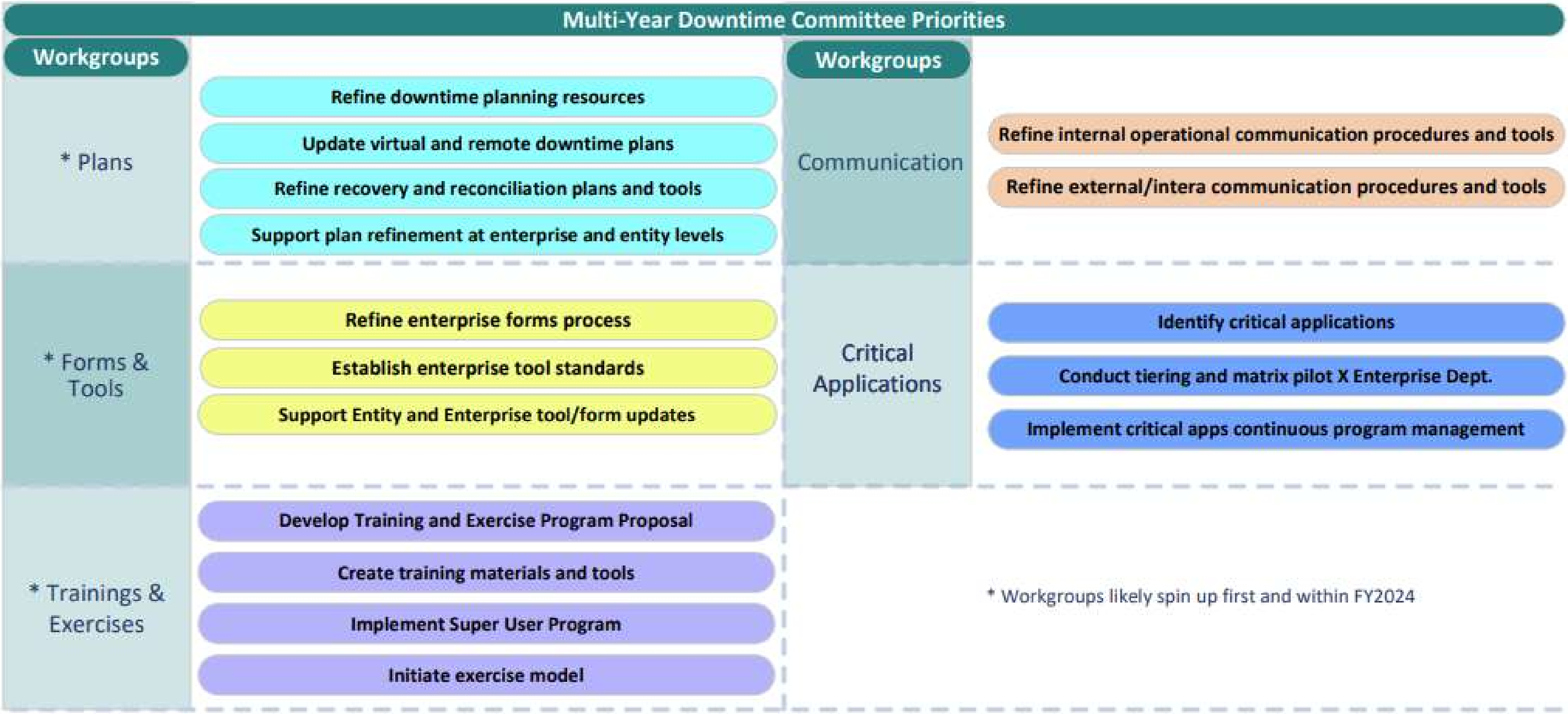
Conduct continuous improvements

- Leverage experience and After-Action Reviews (AAR) from training, exercise and real-world events to identify opportunities for improvement.

Facilitate risk mitigation efforts

- Guide downtime readiness direction and mitigation activities across the enterprise.
- Weigh risks and their anticipated impacts to support unified coordination.

High Level Downtime Committee Roadmap



Multi-Year Downtime Committee Priorities

Workgroups

* Plans

- Refine downtime planning resources
- Update virtual and remote downtime plans
- Refine recovery and reconciliation plans and tools
- Support plan refinement at enterprise and entity levels

* Forms & Tools

- Refine enterprise forms process
- Establish enterprise tool standards
- Support Entity and Enterprise tool/form updates

* Trainings & Exercises

- Develop Training and Exercise Program Proposal
- Create training materials and tools
- Implement Super User Program
- Initiate exercise model

Workgroups

Communication

- Refine internal operational communication procedures and tools
- Refine external/intera communication procedures and tools

Critical Applications

- Identify critical applications
- Conduct tiering and matrix pilot X Enterprise Dept.
- Implement critical apps continuous program management

* Workgroups likely spin up first and within FY2024

Training

Baseline Downtime Training for Electronic Medical Record –
Basic training combined with in person handling and review of downtime tools and paper forms.

Superuser or Champions Framework –
A select group of individuals/job roles represented in every shift that have an established responsibility to become Downtime Super Users/Champions. These individuals have additional downtime response, recovery, and resource training.

Just In Time Training –
One pagers, off network videos, or checklists available to front line staff to guide initial downtime response and tool usage.

- Goal of a Champions Framework is to balance disruptions to operations and daily workload with ensuring downtime readiness.
  - Ensure a number of individuals on each unit/department/clinic have an enhanced level of training and can support other team members in the event of a downtime.
  - The requirement for enhanced training and their downtime leadership position is incorporated into job responsibilities.
  - Individuals need to be ready to respond but it minimizes the disruption and lift of training and exercise initiatives.

Exercises

Mass General Brigham has conducted several exercises of system/entity response to a cyber-attack.

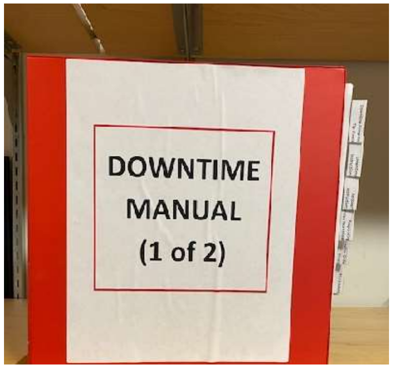
- Front line exercises to ensure readiness:
  - Functional exercises designed to test resiliency of operations
  - Targeted skill drills at the practice/unit/clinic level to ensure front line familiarity with tools and processes
- Executive level decision-making exercises to support our downtime management of operations and decision-making.

These exercises have included the following developments and complications to simulate known real world events and to test multiple aspects of our preparedness and plans:

- Concern over data integrity and equipment
- Operational impacts during prolonged downtime– EHR and telecom downtime, medication order issues, discharges delayed, dietary orders not accessible, capacity challenges/flow of care, etc
- Local and national media attention
- Patient and family relations concerns
- Interaction with external partners and government agencies
- Complexity of recovery and reconciliation

Downtime Toolkit

- Downtime Paper Forms
  - — Recommended minimum 2 days of highest utilized forms
- Tip Sheets for Key Tools:
  - — Epic Read – Only
  - — Downtime BCA Computer
- Enterprise Downtime Procedures
  - — Clinical Minimum Data Set for Reconciliation
  - — Downtime Scenarios Grid (i.e. tool mapped to scenario)
- Site Downtime Procedures
  - — By Patient Care Area (Inpatient/ED, Periop, Ambulatory)
  - — List of common emergency telephone/fax numbers, pagers, red phones, etc.
  - — Instructions for obtaining paper prescription pads
- Optional:
  - — All downtime paper forms on thumb drive
  - — Blank patient (Avery) labels and blank patient wristbands



Continuity and Capability Based Approach

- Given the complexity of healthcare and operations, we cannot possibly plan for every scenario or variation.
- A capabilities based approach to planning is critical to ensuring resiliency against all disruptions – including primary impacts to cascading impacts from third party risk.
  - Integrates an understanding of dependencies: Staff, Supplies, Space and Systems (4S's)
  - Rooted in continuity planning
  - Supports prioritization of resources and restoration

In Closing

Downtime readiness is critical to enhance resiliency of healthcare operations across different types and sizes of organizations.

Key Takeaways

- Cyber hazards/attacks must be integrated into all-hazards plans and exercises.
- Being prepared and knowing how to respond is critical: training should be required and integrated into operations.
- Early collaboration, including outside of response, across departments is critical to successful preparedness and response *during* a cyber incident.
- The tools and programs discussed today are scalable to fit your need and organization size.

Mass General Brigham