Access the recording here:
https://register.gotowebinar.com/recording/1576685793682355463

Access speaker bios here: https://files.asprtracie.hhs.gov/documents/healthcare-operations-speaker-series-cybersecurity-considerations-speaker-bios.pdf

TRACIE
HEALTHCARE EMERGENCY PREPAREDNESS INFORMATION GATEWAY

Healthcare Operations Considerations Speaker Series

February 2021

ASPR
ASSISTANT SECRETARY FOR PREPAREDNESS AND RESPONSE

Healthcare System Cybersecurity: Readiness and Response Considerations

Access the report here: https://files.asprtracie.hhs.gov/documents/aspr-tracie-healthcare-system-cybersercurity-readiness-response.pdf

Acknowledgements

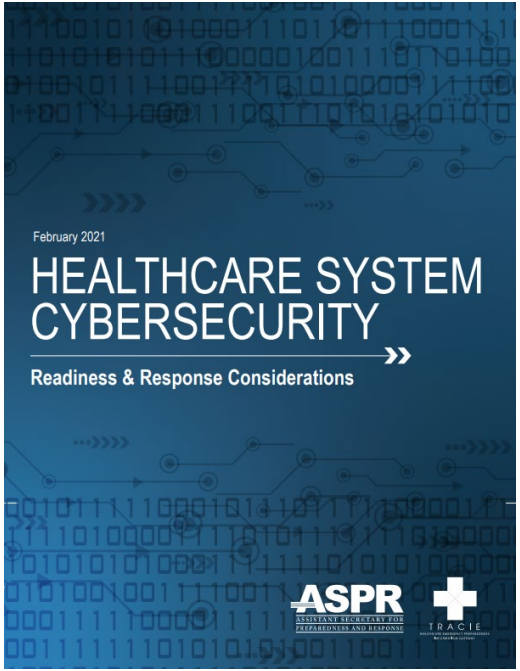
Nebraska Medicine, MedStar Health, and ASPR TRACIE SMEs

ASPR TRACIE Cybersecurity Resources

- Cybersecurity Topic Collection
- Exchange Issue 2: Cybersecurity and Cyber Hygiene
- Cybersecurity and Healthcare Facilities Video

Why Cybersecurity and Healthcare

- Cyberattacks were identified as top threat in healthcare system Hazard Vulnerability Analyses (HVAs)
- Recent attacks highlighted the need for a comprehensive cybersecurity document tailored for healthcare operations
- Lessons learned and best practices should be shared across the health sector to improve preparedness and response efforts



TRACIE

HEALTHCARE EMERGENCY PREPAREDNESS INFORMATION GATEWAY

Craig DeAtley, PA-C
Director, Institute for Public Health Emergency Readiness,
MedStar Washington Hospital Center

ASPR
ASSISTANT SECRETARY FOR PREPAREDNESS AND RESPONSE

Scope of Resource

Specific Focus

- Impact of a large-scale cyberattack on a healthcare facility/organization
- Disruptions on routine healthcare operations across clinical and non-clinical departments
- Ability to maintain quality patient care and critical business practices

Limited Coverage

- Overview of general cybersecurity practices, industry standards
- Does not cover in depth IT protocol, medical device/equipment protection
- Additional information available in Resources and Appendix sections

Structure: Sections & Navigation

QUICK LINKS

- Left hand navigation bar
- Table of contents layout
- Easier topic identification

PREPAREDNESS & MITIGATION

- Standard security practices
- System evaluations
- Readiness activities

RESPONSE

- Assessing impact
- Incident command
- Downtime procedures

RECOVERY

- Long-term effects
- Resumption of services
- Demobilization

QUICK LINKS
PREPAREDNESS & MITIGATION
RESPONSE
RECOVERY

INTRODUCTION

As part of our nation's critical infrastructure, healthcare facilities large and small must be proactive and move quickly to protect themselves from cyberattacks that could directly impact the health and safety of patients and the community at large. According to medical health experts experienced in cybersecurity preparedness, cyberattacks are identified as the top threat in many healthcare systems' annual Hazard Vulnerability Analyses (HVA). The federal government, with other public and private sector partners, has worked diligently to defend against the growing number of cyberattacks on the healthcare industry.

RELATED RESOURCES

Cybersecurity Topic Collection

Cybersecurity and Cyber Hygiene (Issue 2 of *The Exchange*)

Cybersecurity and Healthcare Facilities (Webinar)

Lessons Learned from the Medstar Health System Outage

The U.S. Department of Health and Human Services (HHS) Office of the Assistant Secretary for Preparedness and Response (ASPR) has sponsored the ASPR Technical Resources, Assistance Center, and Information Exchange (TRACIE) since 2015. The goal of ASPR TRACIE is to fill gaps in healthcare system preparedness capabilities by providing timely, innovative ways to share information and promising practices during planning efforts. ASPR TRACIE designed this resource to help healthcare facilities, and the systems they may be a part of, understand the roles and responsibilities of stakeholders before, during, and after a cyber incident.[1] Information within this document is specifically related to the effects of a cyber incident on the healthcare operational environment, specifically the ability to effectively care for patients and maintain business practices and readiness during such an event. While the focus of this document is on disruptions associated with a large-scale cyberattack, many strategies and principles outlined are relevant to a range of cybersecurity incidents and healthcare facilities.

This document cites general cybersecurity practices; additional resources that cover more complex cybersecurity practices (e.g., those associated with medical devices) can be found in the resources section and Appendix.

ASPR TRACIE created the following ***checklists*** for operational use:

Hospital Downtime Operations Checklist

Hospital Downtime Preparedness Checklist

Cyber Incident Response Checklist

Cyber Incident System Restoration Checklist

[1]For purposes of this resource, a cyber incident is defined as "Actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and/or the information residing therein" (NIST).

2 **ASPR TRACIE** HEALTHCARE SYSTEM CYBERSECURITY

Structure: Additional Resources

- Operational Checklists (*Links*)
- Promising Practices (*Call Out Box*)
- Related Resources (*End*)
- Appendix (*Link*)
- Other ASPR TRACIE Products (*Link*)

These checklists can help healthcare facility personnel prepare for and manage downtime due to cyber incidents:

Hospital Downtime Preparedness Checklist

Hospital Downtime Operations Checklist

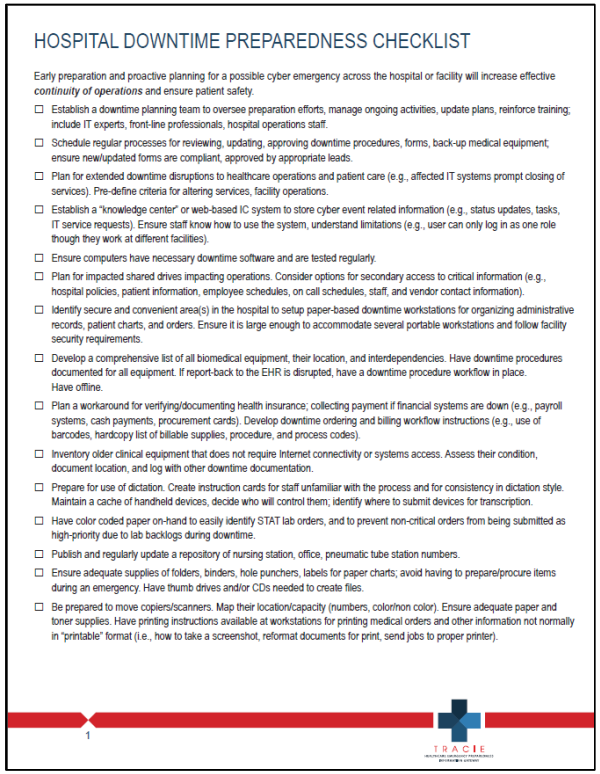
Operational Checklists

Critical steps to take when preparing for and functioning within a modified operational state during a cyber incident

- ***Hospital Downtime Preparedness Checklist***
- ***Hospital Downtime Operations Checklist***

Strategies to consider to ensure effective response and recovery from a cyber incident

- ***Cyber Incident Response Checklist***
- ***System Restoration Checklist***



HOSPITAL DOWNTIME PREPAREDNESS CHECKLIST

Early preparation and proactive planning for a possible cyber emergency across the hospital or facility will increase effective *continuity of operations* and ensure patient safety.

- ☐ Establish a downtime planning team to oversee preparation efforts, manage ongoing activities, update plans, reinforce training; include IT experts, front-line professionals, hospital operations staff.
- ☐ Schedule regular processes for reviewing, updating, approving downtime procedures, forms, back-up medical equipment; ensure new/updated forms are compliant, approved by appropriate leads.
- ☐ Plan for extended downtime disruptions to healthcare operations and patient care (e.g., affected IT systems prompt closing of services). Pre-define criteria for altering services, facility operations.
- ☐ Establish a "knowledge center" or web-based IC system to store cyber event related information (e.g., status updates, tasks, IT service requests). Ensure staff know how to use the system, understand limitations (e.g., user can only log in as one role though they work at different facilities).
- ☐ Ensure computers have necessary downtime software and are tested regularly.
- ☐ Plan for impacted shared drives impacting operations. Consider options for secondary access to critical information (e.g., hospital policies, patient information, employee schedules, on call schedules, staff, and vendor contact information).
- ☐ Identify secure and convenient area(s) in the hospital to setup paper-based downtime workstations for organizing administrative records, patient charts, and orders. Ensure it is large enough to accommodate several portable workstations and follow facility security requirements.
- ☐ Develop a comprehensive list of all biomedical equipment, their location, and interdependencies. Have downtime procedures documented for all equipment. If report-back to the EHR is disrupted, have a downtime procedure workflow in place. Have offline.
- ☐ Plan a workaround for verifying/documenting health insurance; collecting payment if financial systems are down (e.g., payroll systems, cash payments, procurement cards). Develop downtime ordering and billing workflow instructions (e.g., use of barcodes, hardcopy list of billable supplies, procedure, and process codes).
- ☐ Inventory older clinical equipment that does not require Internet connectivity or systems access. Assess their condition, document location, and log with other downtime documentation.
- ☐ Prepare for use of dictation. Create instruction cards for staff unfamiliar with the process and for consistency in dictation style. Maintain a cache of handheld devices, decide who will control them; identify where to submit devices for transcription.
- ☐ Have color coded paper on-hand to easily identify STAT lab orders, and to prevent non-critical orders from being submitted as high-priority due to lab backlogs during downtime.
- ☐ Publish and regularly update a repository of nursing station, office, pneumatic tube station numbers.
- ☐ Ensure adequate supplies of folders, binders, hole punchers, labels for paper charts; avoid having to prepare/procure items during an emergency. Have thumb drives and/or CDs needed to create files.
- ☐ Be prepared to move copiers/scanners. Map their location/capacity (numbers, color/non color). Ensure adequate paper and toner supplies. Have printing instructions available at workstations for printing medical orders and other information not normally in "printable" format (i.e., how to take a screenshot, reformat documents for print, send jobs to proper printer).

1

TRACIE

Promising Practices

Collection of lessons learned and best practices to help ensure readiness and effective continuity of operations in the event of a cyberattack

- ***IT Readiness Promising Practices***
- ***Exercise Promising Practices***
- ***Clinical Promising Practices***
- ***Downtime Documentation Promising Practices***
- ***Downtime Financial Promising Practices***

Clinical Promising Practices

- ***Establish a process for how orders will be created, collected, and communicated to hospital runners***. For departments such as food service and cleaning that will likely remain busy, avoid having departments call-in their orders unless there is a designated person to answer the phone and coordinate requests. Create a standard process to log, reference, and close orders.
- ***Set up workstations for collecting, organizing, and storing manually written medical records***. Organize files so that it is easy to identify patients based on location within the unit/hospital.
- Ensure departments use the proper Medical Record Numbers (MRNs) (i.e., designated downtime MRNs) versus previous MRNs to avoid conflict and confusion.
- ***Create workarounds in case of limited access to business continuity data*** and information such as station reports/patient information. Having IT staff focused on accessing patient information can be resource intensive, impacting recovery.

Section 1. Preparedness & Mitigation

Cybersecurity Readiness

- Standard IT preparedness principles
- Facility considerations based on size, need (federal services/support)

Routine Mitigation

- Ongoing system and infrastructure protection practices
- Incident management planning (emergency management plans/structures)
- Common facility/administrative considerations (alerting, communications, legal)

IT Evaluations & Exercises

- Identify and mission critical assets/functions, workflows for prioritization
- Review routine exercises used to inform readiness (drills, white hat)

Downtime Principles

- Properly preparing for downtime (defining downtime, documentation needs)
- Preparing workforce for disruptions associated with downtime

TRACIE

HEALTHCARE EMERGENCY PREPAREDNESS INFORMATION GATEWAY

Shelly Schwedhelm, MSN, RN, NEA-BC
Executive Director, Emergency Management and Biopreparedness, Nebraska Medicine and Global Center for Health Security, Nebraska Medicine

ASPR
ASSISTANT SECRETARY FOR PREPAREDNESS AND RESPONSE

Section 2. Response

Assessing Impact

- Identifying a cyber incident
- Determining scope/impact level
- Understanding triggers and alerting

Incident Command Principles

- Determine proper response protocol
- Implement the Incident Management Team (IMT)/structure
- Ensure collaboration/inclusion across departments, facilities
- Communicate/share information related to the incident

Workforce Resilience

- Staffing adjustments
- Additional support needs
- Gaps in patient care/services

Section 2. Response

Downtime Procedures

- Downtime forms
- Downtime operations
- Downtime financial practices

Operational Considerations

- Consistency in response practices
- Handling of Electronic Health Records, patient data
- New communication channels (email/phone disrupted, web-based incident management system, radios)
- Disruption of medical services, need to reduce patient volume

Clinical Considerations

- Facilitating patient medical orders
- Establishing workstations
- Postponing administrative tasks (hiring, evaluations, HR services)

Section 2. Response (continued)

Communication/Information Sharing

- Implement communication plan
- Manage/coordinate messaging
- Internal communication protocol
- External communication protocol

Facility Security

- Impact to controlled access points
- Workarounds for monitoring patients (mother/child, psychiatric departments)
- New security protocol (security officers, sign-in sheets, visitor restrictions)
- Securing access to restricted areas (drug cabinets, supply areas)

Safety Considerations

- Proper engagement and protocol to report incidents
- Safety form workflow
- Emphasis on medical order safety protocol
- Patient verification

Section 3. Recovery

Recovery Principles

- Timeline to recovery
- Continued staff schedule adjustments
- Status updates

Resumption of Medical Services/Equipment

- Resume services based on previous assessments
- Validate operational function of devices/equipment
- Resume suspended in-patient procedures

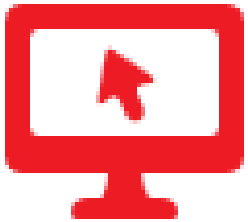
Records Reconciliation

- Financial best practices
- Reconstitution of medical records

Demobilization

- Criteria for de-escalation
- Post incident documentation/activities

Contact ASPR TRACIE



asprtracie.hhs.gov

1-844-5-TRACIE

askasprtracie@hhs.gov