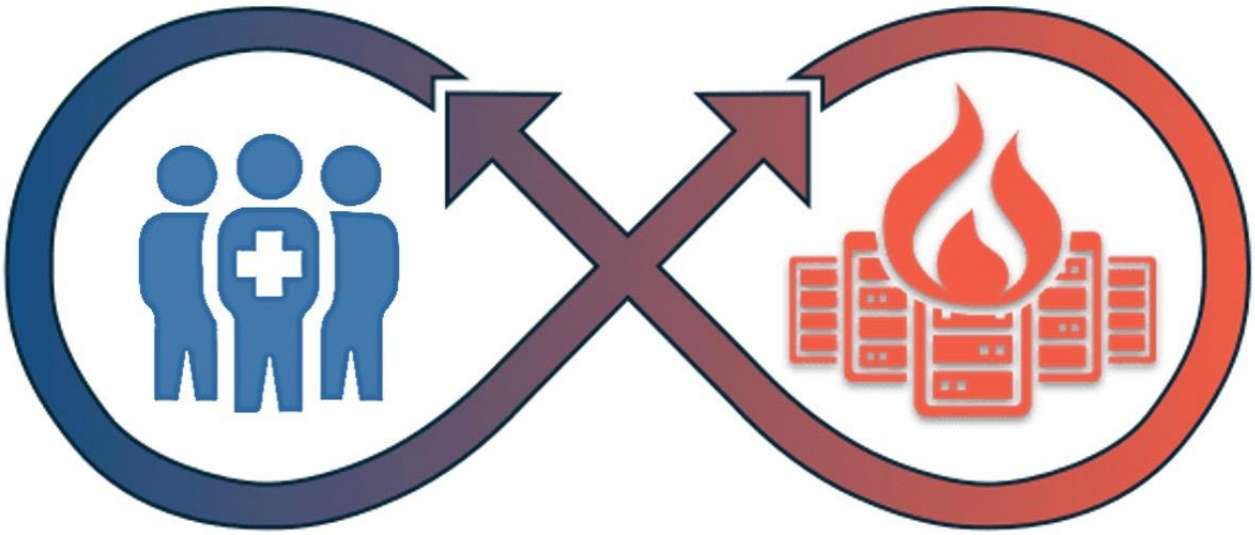
Health Sector Coordinating Council
Cybersecurity Working Group

Manage Risks | Respond & Recover | Measure Effectiveness

Health Industry Cybersecurity -

Operational Continuity – Cyber Incident (OCCI)



MAY 2022

Table of Contents

About the OCCI Checklist

This Operational Continuity-Cyber Incident (OCCI) checklist is intended to provide a flexible template for operational staff and executive management to respond to and recover from an extended enterprise outage due to a serious cyber-attack. Its suggested operational structures and tasks can be modified or refined according to an organization's size, resources, complexity and capabilities. It represents the best collective thinking of private-sector cybersecurity and emergency management executives of the HSCC Incident Response/Business Continuity (IRBC) Task Group of the Health Sector Coordinating Council's Cybersecurity Working Group (CWG). It is not associated in any way with any regulatory compliance program.

Development Process

As the IRBC Task Group was being stood up, it was clear that geopolitical tensions from the Ukraine-Russia conflict were introducing a higher threat level to the health sector, calling for heightened awareness and immediate preparations against potential disruptions to health care delivery. Accordingly, through the IRBC TG the HSCC created this tactical checklist with an accelerated development cycle to anticipate the potential for an extended outage in the event of direct cyber-attacks or collateral fallout and put it into the hands of our stakeholders as quickly as possible. This is a living document that can be refined using stakeholder feedback with operational experience.

Organization

This checklist is organized into role-based modules to align with the Incident Command System. Specific actions recommended for each role are enumerated in the left column of the table, not as a prioritized sequencing of actions, but for easy reference during review or execution.

As enterprises organize their cybersecurity and emergency management roles with varying structures, this checklist attempts to generalize as much as possible to scale and align with those variations. Users will naturally tailor this checklist to fit their specific organizational structures or may adopt some of the recommendations as new additions to their operating procedures.

The HSCC intends to review and update this reference as experience and recommended improvements dictate. We encourage stakeholders who have adopted some or all of the recommendation to provide feedback about its use and help contribute to effective operational continuity procedures. Please send your comments at any time to: Feedback@HealthSectorCouncil.org.

About the Health Sector Coordinating Council

The Healthcare and Public Health Sector Coordinating Council (HSCC) is a coalition of private-sector critical healthcare infrastructure entities organized under the National Infrastructure Protection Plan to partner with and advise the government in the identification and mitigation of strategic threats and vulnerabilities facing the sector's

ability to deliver services and assets to the public. The HSCC Cybersecurity Working Group (CWG) is the largest HSCC working group of more than 400 healthcare providers, pharmaceutical and medtech companies, payers and health IT entities partnering with government to identify and mitigate cyber threats to health data and research, systems, manufacturing and patient care. The CWG membership collaboratively develops and publishes freely-available healthcare cybersecurity best practices and policy recommendations, and produces outreach and communications programs emphasizing the imperative that cyber safety is patient safety.

For more information about joining the HSCC as a healthcare entity, please visit https://healthsectorcouncil.org/contact/.

Response Guideline – Cybersecurity/Technology System Prolonged Massive Disruption or Outage

This checklist outlines recommended initial (first 12 hours) actions and considerations during cybersecurity incidents. Command positions should be activated as they are needed. If a command position is not activated, actions fall to the Incident Commander and can be delegated as appropriate. Position activation may depend on staff availability or the size and scope of the incident.

Based on assessment by CIO, CISO, and senior leadership, incident command may be activated Threshold for activation:

A prolonged massive disruption meets or has the potential to meet any of the following:

a. Patient safety and/or member service impacts
b. Large-scale clinical workflow, patient care, and/or member service impacts
c. Implementation of preventative defenses that could impact clinical workflow

Incident Commander

Role: Provides overall strategic direction on all site-specific response actions and activities.

1.1 Identify Incident scope and obtain situational awareness

- Identify Scope – One site/multiple sites/Isolated outage/full network outage
  - Assume it is a malicious (cybersecurity) incident until proven otherwise
- Situational awareness – operational, business, and clinical impacts

1.2 Establish a cadence and process for coordination with IS/IT and Cyber Security

- Consider command center coordination or unified command based on organizational structure *(Hospital, IS/IT, and Cybersecurity Command)*

1.3 Activate applicable continuity and downtime plan(s)

- If plans do not exist or are not functional, rapidly identify critical services and create a plan to continue/sustain services

1.4 Communicate activation of downtime plans to inform operational changes

- Consider use of overhead paging, mass notification system, etc.

1.5 Approve recommendations from Operations relative to:

- Scaling services
- Pausing services
- Initiating diversionary status

1.6 Address incident need by activating additional resources

1.7 Understand upstream and downstream impact(s) to partner organizations.

Communicate as appropriate.

- Community Connect
- Other health systems
- Community partners (e.g., SNF, LTAC, EMS)

1.8 Establish cadence for ongoing impact assessment and briefing (e.g., operational periods)

Medical-Technical Specialist (Subject Matter Expert/Advisor)

Role: Subject matter expert(s) who advises the Incident Commander or Section Chief on issues related to response; provides understanding and communicates specific impact and recommendations given their area of expertise.

Given the complexity and scope of this response, it is recommended to activate a Medical Technical Specialist Team

Note: This could alternatively be activated as a branch within Intelligence (IT/IS) Section Chief

2.1 Cybersecurity:

- Collaborate with IS/IT to contain the spread of malicious activity
- Perform analysis and forensics as needed to isolate the threat
- Identify impacted systems – consider Clinical Engineering, Lab, Pharmacy, Imaging, etc.
- Request additional expertise based on capability of internal team

2.2 Risk Management/Regulatory & Compliance/Legal:

- Assess the need for and advise the Incident Commander regarding changes to risk management and loss prevention program policies as appropriate to response
- Consider activation of Cyber Insurance policy and procedures
- Consider extortion components
- Consider initiation of digital forensics/incident response (DFIR)
- Gather invoices to support non-cyber-related claim file process
- Complete other reporting requirements
- Provide notification to regulatory agencies as appropriate

2.3 CNO/CMO/Clinical Leader/Safety & Quality:

- Advise on issues with ethical implications

- Understand and communicate clinical impact(s) to inform waivers, contingency care or Crisis Standards of Care activation
- Coordinate with Medical Staff Office, Transfer Center, and Telehealth Services for needs relative to rapid credentialing, privileging, and reduction/expansion of services
- Consider special populations, including pediatrics, transplant, behavioral medicine, etc.

Public Information Officer

Role: Serve as the conduit for information to internal and external stakeholders, including site personnel, visitors and families, and the news media, as approved by Cybersecurity, IS/IT Section Chief and the Incident Commander.

3.1 Receive briefing from Incident Commander on situation and status

3.2 Establish cadence for coordination with cybersecurity leadership or Med-Tech Specialist for collaboration on internal and external communications

3.3 If appropriate, activate crisis communication plan

Rapidly develop **internal** communication for approval by Incident Commander

- Identify an internal spokesperson and provide guidance as appropriate
- Establish a plan to communicate to current and oncoming staff
  - Recommend operations section leverage local leaders for local guidance
  - Include providers in scope of communication
  - Note: consider that internal communication rapidly becomes external
- Hospital leadership notification (may depend on size and scope facility)
- Develop talking points for staff in patient- or public-facing departments
  - Note: this should include phone-related services
- Identify a mechanism and cadence for executive communication
  - Consider communication to executives/board of trustees

3.4 Work with Operations Section Chief and IT/IS Section Chief to support activation of redundant communications, if available

- If needed, collect contact information for command and general staff and create communication directory

3.5 Develop **external** communication for approval by Incident Commander

- Prepare instructions for patients, family, and community members
  - Consider alternate phone numbers to contact site services
  - Consider access to online records or tele-services
  - Consider the impact to internal Wi-Fi connectivity
  - Consider family members of onsite staff
- Coordinate with Liaison and Cybersecurity to ensure external contact alignment and appropriate notification to approved partner(s)

3.6 Collaborate with Cyber Security to develop a **media and PR strategy**

- Note: during a cybersecurity incident, **providing information to the public may create additional vulnerabilities**. If a criminal investigation is possible, coordination with law enforcement will be required to identify what details may be disclosed
- Identify the scope of information that can be shared and to what audience
- Monitor social media and other media reports
- Identify if and how information may be provided to media outlets
- Establish media staging area

Liaison

Role: Function as the incident contact for the Command Center for representatives from other agencies.

4.1 Coordinate external partner communication with PIO, Med-Tech, IS/IT Section Chief

- Note: If not activating Med-Tech Section, ensure coordination with Cybersecurity

4.2 Notify external agencies or partners as appropriate

- Emergency Medical Services (EMS)
- Local and state dispatch centers
- Municipal Emergency Management
- Government Agencies
- Health Department
- Healthcare coalition

4.3 Consider pursuit of disaster declaration

Safety Officer

Role: Identify, monitor, and mitigate safety risks to patients, staff, and visitors during a prolonged large-scale outage

5.1 Understand and address safety impacts based on incident. These may include:

- Staffing
- Central and remote patient monitoring
- Telehealth services
- Duress/Distress/panic alarm/nurse call alerting buttons or systems
- Imaging (readability)
- Pharmacy (dispensing and safety checks in the ERM/ADM)
- Environmental controls
    - Refrigeration, temperature tracking
    - Sterile processing
    - HVAC, humidity, air exchange
    - Clinical impacts to lab, pharmacy, tissue
    - Morgue/decedent management
- Access control systems: physical access and CCTV
- Other network-reliant systems

- Tube system, lab devices, text paging, radio repeaters
- Implement or activate analogue process(es) for safety reporting
  - Patient safety reporting
  - Employee safety reporting

5.2 Prepare to receive external agencies direct to command center

- Activate temporary identification and understand access controls

Operations Section Chief

Role: Develop and recommend strategies and tactics to continue clinical and non-clinical operations for the duration of the incident response and for recovery.

6.1 Activate downtime procedures

- Identify safe, alternative processes for patient care based on technical outage
- Initiate downtime processes:
  - Utilize business continuity or downtime computers if available
  - Build paper charts for all patients using information printed from downtime computers or paper downtime forms.
  - Print critical service delivery information (e.g., patient charts, staff schedules, patient schedules)
  - Establish patient and specimen label process
- Note: this could be an extended downtime (days or weeks) – address downtime procedures that need to be refined to support extended downtime
- Establish or implement back charting criteria
- Deploy strike teams to provide just-in-time training and regulatory requirements on downtime charting and documentation

6.2 Activate business continuity plans for clinical and operational services

Conduct ongoing assessment of impacts to staff, space, supplies and equipment across:

- ED/Trauma
- Critical Care
- Acute Care
- Women's & Newborn
- Surgical Services
- Pediatric Care
- Air medical services
- Telehealth
- Transfer Center
- Behavioral Health
- Oncology
- Transplant
- Staffing needs

Escalate to appropriate section chief(s)

6.3 Provide recommendations for scaling back services

- Non-urgent elective procedures
- Outpatient services

6.4 Provide recommendations for delaying services

- Non-urgent elective procedures
- Outpatient services

6.5 Provide recommendations for altering

- Laboratory Services (e.g., test volumes, specimen processing, outsourcing)
- Imaging Services (e.g., time-sensitive or emergent only)
- Pharmacy Services (e.g., decrease outpatient services)
- Rehabilitative Services

Planning Section Chief

Role: Oversee all incident related documentation regarding incident operations and resource management, initiate long range planning; conduct planning meetings; prepare the Incident Action Plan (IAP) for each operational period.

7.1 In collaboration with the Incident Commander, use the Planning P to:

1. Establish operational periods
2. Record incident objectives
3. Develop incident Action Plan (IAP)
4. Schedule and execute appropriate briefings and reviews

7.2 Receive and collate data from local team status forms

- Prioritize critical areas and needs
- Develop situation report for command staff

7.3 Contact local areas who did not report status

7.4 Prepare for patient and personnel tracking in digital and printed form

- Staffing logs
- Patient logs

7.5 Prepare staffing plan and recommendations to support operations

- Support staff may be needed to support the outage – engage staffing office
  - Consider experienced staff/champions skilled in downtime procedures
- Consider extended needs which may require:
  - Runners
  - Transporters
  - Nursing ratios

- Redeployment
- Remote work: continuation vs. site needs
- Onsite support: loss of telehealth or other services
- Engaging Liaison section for external resource support

7.6	In collaboration with Operations Section Chief and PIO, develop process for contacting patients and family regarding alterations to procedures and appointments

Finance Section Chief

Role: Monitor the utilization of financial assets and the accounting for financial expenditures; supervise the documentation of expenditures and cost reimbursement activities.

8.1	Track costs, expenditures, and revenue impacts
8.2	Develop contingency strategies for impacts to financial data • Engage appropriate section chief(s) to communicate changes
8.3	Consider establishing a cost center specific to the incident
8.4	Gather invoices to support non-cyber-related claim file processes
8.5	Consider modifying restrictions for purchase card or corporate card limits
8.6	Develop and communicate contingency strategies for impacts to retail or point-of-sale systems
8.7	Facilitate contracting for other emergency support as needed
8.8	Oversee manual payroll and timekeeping processes as needed
8.9	Coordinate with outside vendors for delayed or manual payment processes
8.10	Partner with Med-Tech Section on insurance and reimbursement documentation

Logistics Section Chief

Role: Organize and direct the service and support activities needed to ensure material needs for the site's response to an incident are available when needed.

9.1	Identify any potential disruptions to critical infrastructure and priority services
9.2	Regularly evaluate electrical system performance • Consider network-reliant systems (e.g., tube system, temperature controls, etc) • Deploy additional staff to manually monitor systems reliant on the network (HVAC, humidity, etc.) • If the fire suppression system is reliant on the technical network, activate a fire watch
9.3	Partner with IS/IT to identify communication redundancies for:

	• Translation services (services offered previously via telehealth may need to be brought on site) • Visitors, family members, clergy, or vendors (e.g., phone or video calls, end of life care)
9.4	Ensure food and hydration is available; consider patients, staff, visitors, and command center
9.5	Prepare for radio deployment: • Charge radios, batteries, and additional batteries • Provide just-in-time training on radio use • Oversee sign-out sheet to track all deployed radios
9.6	Ensure adequate downtime supplies: paper, toner, pencils, pens, stationary, forms, etc. Order additional supplies as needed
9.7	Assess impacts to materials management and ordering processes • Implement manual inventory and ordering processes for supply chain management • Implement a manual process for distribution, supply chain, and redistribution of clinical and operational supplies • Ensure availability of durable medical equipment • Ensure availability of oxygen • Ensure availability of pharmaceuticals
9.8	Deploy Environment of Care teams to evaluate contingency needs • Clinical Engineering/Health Technology Management • Environmental Services • Facilities/Maintenance/Engineering • Industrial Hygiene • Infection/Prevention • Security
9.9	Assess ability to source additional technical equipment for end users (laptops, tablets, etc.)
9.10	Redeploy excess staff to support operations
9.11	Establish Labor Pool or coordinated process to redeploy staff • Note: credentials and competency must be accounted for • Provide instructions for manual timekeeping
9.12	Identify staff resiliency resources (EAP, mental health, etc.) for extended incident support

Intelligence (IS/IT) Section Chief

Role: Provide technical response, continuity, and recovery recommendations; partner with cybersecurity to inform incident response decisions and activities. Coordinates intelligence and investigation efforts.

Note: For this incident, this position should be filled with IS/IT professionals

If using an internal unified command structure, consider removing Cybersecurity from Med-Tech Section and placing below

10.1	Address potential IS/IT/Cybersecurity staffing needs and establish staff rotation schedule
10.2	Address any qualifications or security clearance necessary based on incident complexity
10.3	Establish a cadence with cybersecurity for regular situation updates to inform command • Communicate scope and severity of disruption • Identify and communicate upstream and downstream impacts • Support identification and implementation of safe, alternate processes • Assist with restoration of technology systems
10.4	Coordinate with Clinical Engineering/Health Technology Management to understand: • Impacts • Data storage limits to inform downtime processes
10.5	Collaborate with Cybersecurity to understand scope of disruption and potential for cyberattack
10.6	Consider activating unified command with a cyber command structure (cyber, legal, exec) to collaborate on sensitive decisions. (Note: this may be achieved via the Med-Tech Section) • Activate Cyber Insurance Policy and procedures • Coordinate Legal and Risk Management activities • Consider ransomware payment process
10.7	Identify the impact on the following systems: • Bedside care: monitoring, telemetry, pumps, nurse call • Building systems (e.g., tube system, temperature tracking, badge access) • Electronic health record (HER) • Emergency Department/Trauma Services • Imaging • Internet • Intranet • IS Infrastructure • Lab • Network • Revenue Cycle • Surgical Services • Telecom
10.8	At direction of CISO or Cybersecurity leader, consider proactive technical system(s) lockdown) • Consider data center shutdown to prohibit spread • Consider critical systems shutdown to reduce data breach risk

	• Consider shutdown of vendor bi-directional VPN access • Consider shutdown of WAN connections • Consider lockdown of internal network segments • Consider failover to DR, quarantine routers/switches • Scan all backups for integrity
10.9	Consider a recommendation to power down all technology to limit the spread • Engage IS/IT to support network take down/recovery • Engage IS/IT in use of off-network computers for downtime process support
10.10	Establish a process for interim solution, intake, and prioritization
10.11	Provide updates to command staff on estimated length of time until systems can be fully recovered (RTO/RPO in hours/days/weeks)
10.12	Coordinate with Cyber Security on timeline for threat eradication • Note: Reenabling internet/WAN/VPNs may not be possible until threat is eradicated
10.13	Collaborate with Incident Command on restoration and recovery processes • Note: this guide is for the first 12 hours; however, recovery should begin immediately • Identify scope of encryption • Reaffirm recovery time objectives • Validate application recovery priority • Assess critical application dependencies for recovery • Recover critical applications for essential business operations in a timely manner • Recover infrastructure

Acknowledgements

Once the initial scoping for this project was agreed upon by mid-March 2022, the following individuals volunteered as a "Strike Force" to develop this checklist on an accelerated timetable to prepare health delivery organizations and their support systems for the potential of an extended operational outage from a cyber attack. This group met 2-3 times per week over a four-week period to develop this checklist, solicit and adjudicate feedback and format it for ease of use. The HSCC is indebted to their thought leadership, energy and commitment to the operational health of the sector.

Lisa Bisterfeldt

Program Manager Cyber Security
St. Luke's Health System

Mike Caudill

Senior Director, Cyber Security Operations and Incident Response
Duke University Health System

Hazel Chappell

Digital Managing Partner / Executive Business Advisor
Ishca Health

Nate Couture

Network Chief Information Security Officer
The University of Vermont Health Network

Garrett Hagood

Chief Information Security Officer
Coastal Bend Regional Advisory Council

Kirsten Núñez

Emergency Management & Business Continuity
Intermountain Healthcare

Mitchell Parker, MS, MBA, CISSP

VP/Chief Information Security Officer
Indiana University Health

Skip Skivington

Vice President, Healthcare Continuity Management & Support Services
Kaiser Permanente