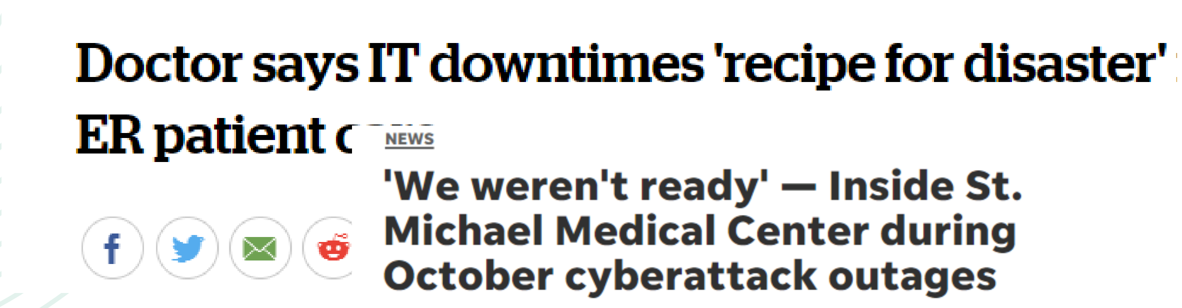
DEVELOPING A RESILIENT RESPONSE

INCREASING CONTINUITY AND RESPONDING TO A CYBER SECURITY ATTACK

Lisa Bisterfeldt
Program Manager, Cyber Resiliency
St. Luke’s Health System

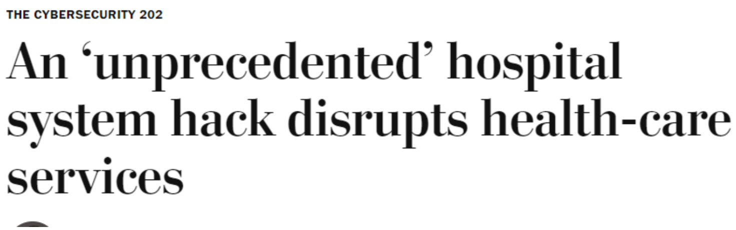


Doctor says IT downtimes 'recipe for disaster'

ER patient c

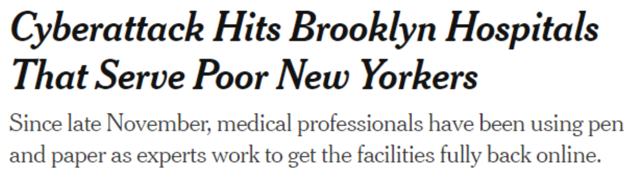
NEWS

'We weren't ready' — Inside St. Michael Medical Center during October cyberattack outages



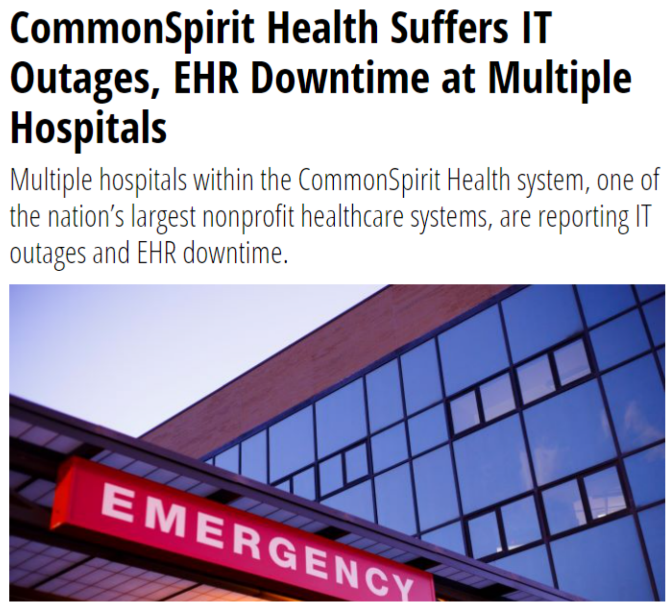
THE CYBERSECURITY 202

An 'unprecedented' hospital system hack disrupts health-care services



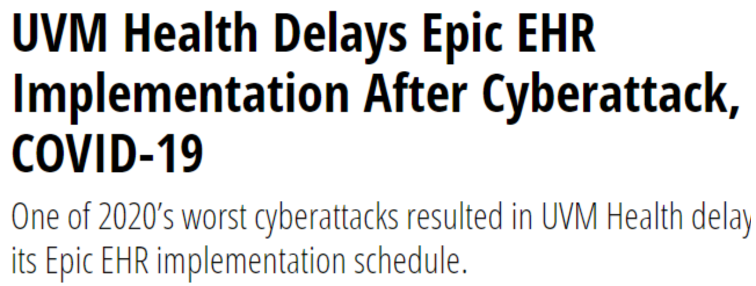
Cyberattack Hits Brooklyn Hospitals That Serve Poor New Yorkers

Since late November, medical professionals have been using pen and paper as experts work to get the facilities fully back online.



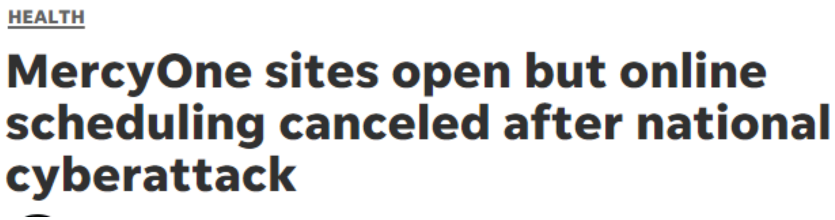
CommonSpirit Health Suffers IT Outages, EHR Downtime at Multiple Hospitals

Multiple hospitals within the CommonSpirit Health system, one of the nation's largest nonprofit healthcare systems, are reporting IT outages and EHR downtime.



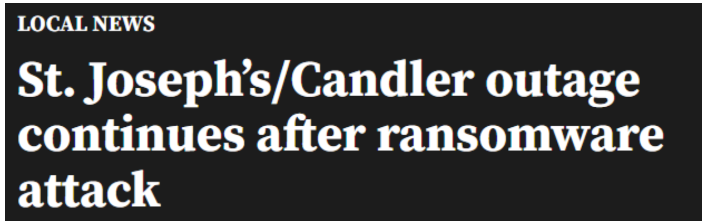
UVM Health Delays Epic EHR Implementation After Cyberattack, COVID-19

One of 2020's worst cyberattacks resulted in UVM Health delay its Epic EHR implementation schedule.



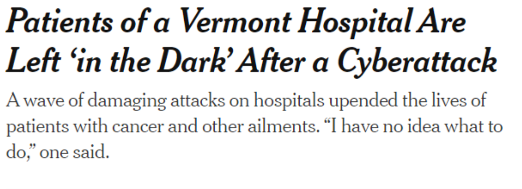
HEALTH

MercyOne sites open but online scheduling canceled after national cyberattack



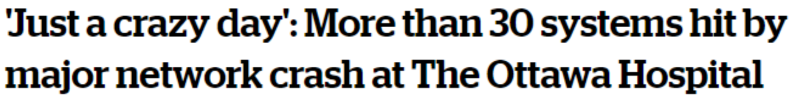
LOCAL NEWS

St. Joseph's/Candler outage continues after ransomware attack

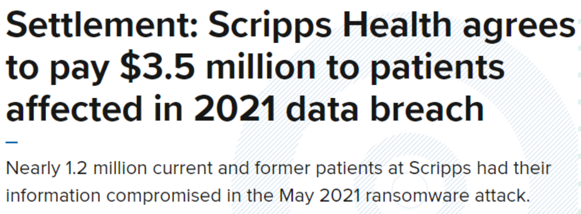


Patients of a Vermont Hospital Are Left 'in the Dark' After a Cyberattack

A wave of damaging attacks on hospitals upended the lives of patients with cancer and other ailments. "I have no idea what to do," one said.

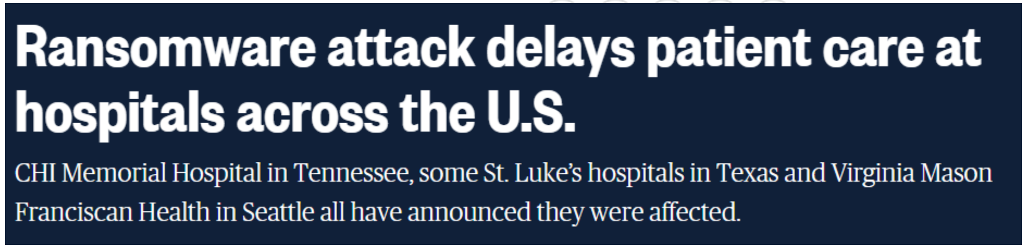


'Just a crazy day': More than 30 systems hit by major network crash at The Ottawa Hospital



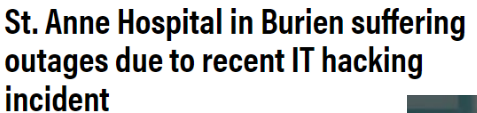
Settlement: Scripps Health agrees to pay $3.5 million to patients affected in 2021 data breach

Nearly 1.2 million current and former patients at Scripps had their information compromised in the May 2021 ransomware attack.

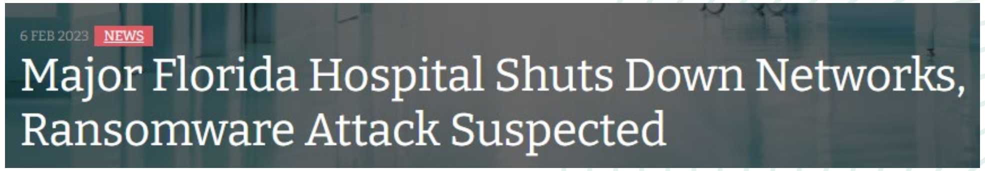


Ransomware attack delays patient care at hospitals across the U.S.

CHI Memorial Hospital in Tennessee, some St. Luke's hospitals in Texas and Virginia Mason Franciscan Health in Seattle all have announced they were affected.



St. Anne Hospital in Burien suffering outages due to recent IT hacking incident



6 FEB 2023 NEWS

Major Florida Hospital Shuts Down Networks, Ransomware Attack Suspected

THE RESULT: EXTENDED DOWNTIMES

Why Healthcare

Technology: Reliance on technology for patient care creates vulnerability

Preparedness: Limited preparedness for large scale cybersecurity attacks

Increased Risk: Operating in downtime creates increased risk

Common Impacts

Complete technical downtime: 1-2 weeks complete

Average recovery time: For applications approximately 21- 56 days

Adjustment to workflow: paper charting, paper order sets, etc.

Network Dependency

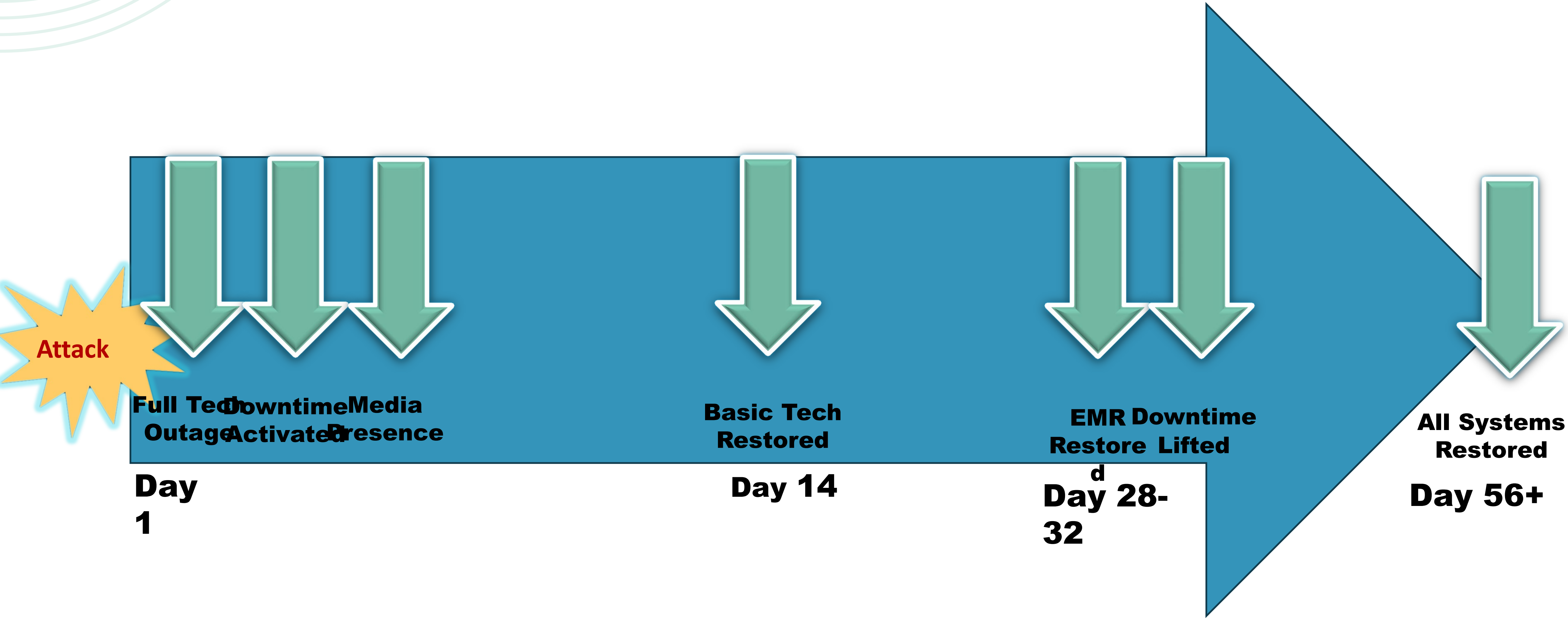
Documentation: EMR, procedure orders, patient education

Priority Applications: pharmaceuticals, imaging, cardiac monitoring, etc.

Resources: supply movement, printers, telephones, email

IMPACT TIMELINE

IT’S A MARATHON, NOT A SPRINT.



Attack

Full Tech Outage

Downtime Activated

Media Presence

Day 1

Basic Tech Restored

Day 14

EMR Restored

Downtime Lifted

Day 28-32

All Systems Restored

Day 56+

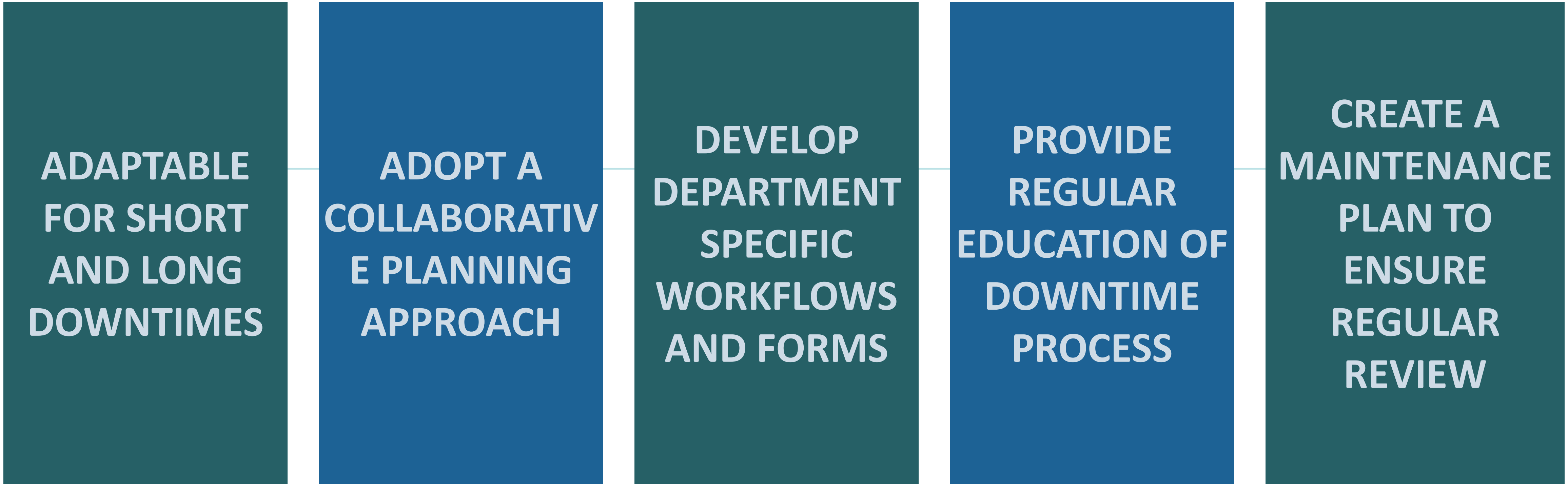
> “ I CANNOT STRESS THIS ENOUGH, EVERY MINUTE WE ARE THERE WE FEEL LIKE WE ARE PLAYING WITH OUR LICENSE ”

Scripps RN following 2021 Cyber Attack

> “ THEY WERE TRYING TO REMEMBER EVERYTHING THEY KNEW ABOUT A PATIENT, BUT NONE OF THAT IS ACCURATE, OUR BRAINS ARE NOT DESIGNED TO BE ELECTRONIC MEDICAL RECORDS. THAT’S NOT SAFE, AND WE ALL KNOW IT. ”

Vermont Health Network RN following 2020 Cyber Attack

INCREASING DOWNTIME MATURITY



ADAPTABLE FOR SHORT AND LONG DOWNTIMES

ADOPT A COLLABORATIVE PLANNING APPROACH

DEVELOP DEPARTMENT SPECIFIC WORKFLOWS AND FORMS

PROVIDE REGULAR EDUCATION OF DOWNTIME PROCESS

CREATE A MAINTENANCE PLAN TO ENSURE REGULAR REVIEW

RESOURCES

Health Sector Coordinating Counsel Cyber Working Group.

- Operational Continuity Cyber Incident (OCCI) Checklist
- Coordinated Healthcare Incident Response Plan (CHIRP)
- From Panic to Plan: Executive Strategies for Handling Cybersecurity Incidents

Health Industry Cybersecurity -

Coordinated Healthcare Incident Response Plan (CHIRP)

HEALTH INDUSTRY CYBERSECURITY

From Panic to Plan: Executive Strategies for Handling Cybersecurity Incidents

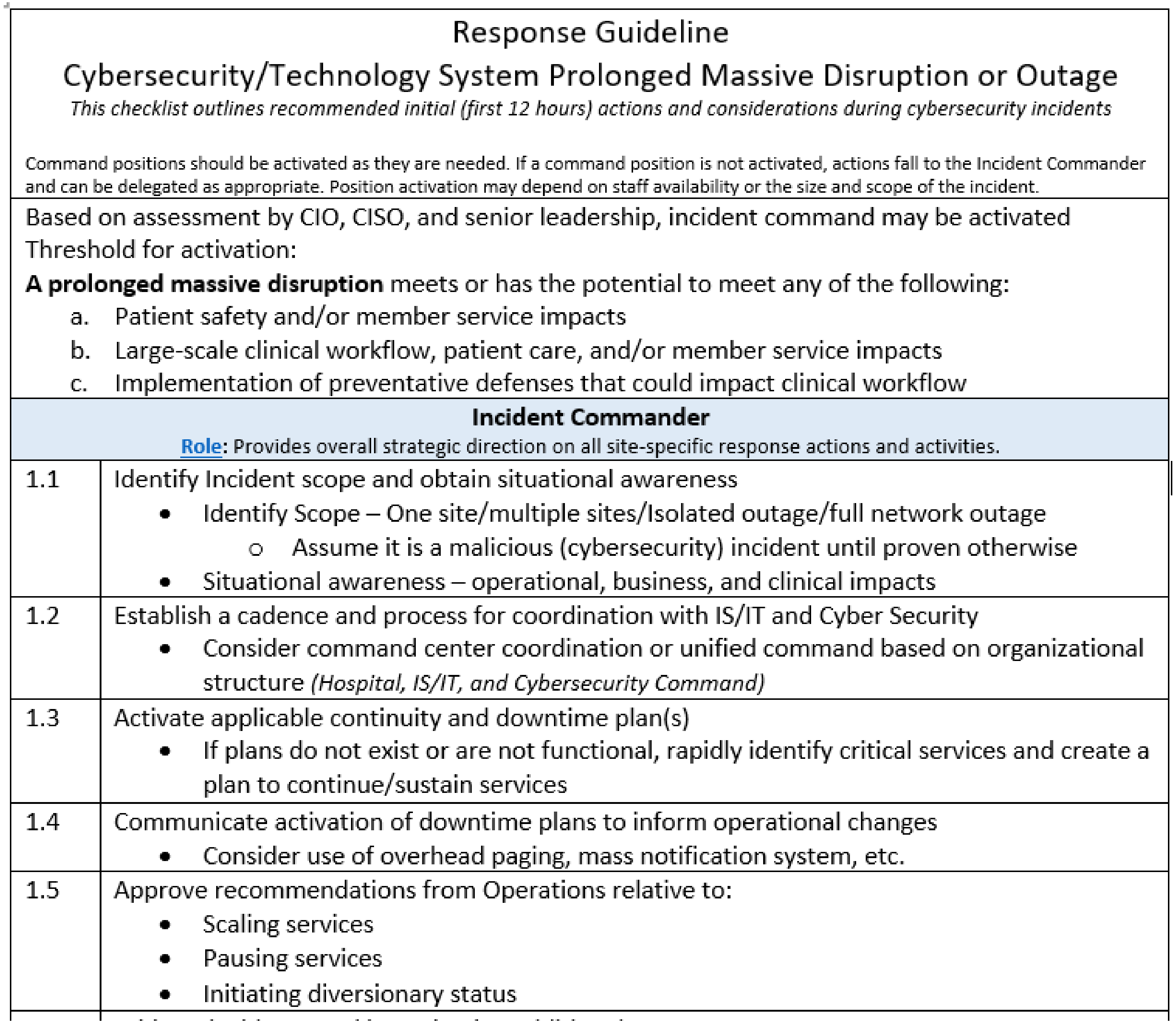
Health Sector Coordinating Council

Cybersecurity Working Group

Health Industry Cybersecurity -

Operational Continuity – Cyber Incident (OCCI)

INCIDENT RESPONSE TOOLS



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

TAKING ACTION

Emergency Operation Plans

- Cybersecurity Annex / Incident Response Plans
- Incident Command Framework
- Communication Plan for Cybersecurity Events
- Collaboration with Cybersecurity, Business Continuity, Disaster Recovery

Training & Education

- Integration of cybersecurity hygiene into regular training.
- Overview of different cybersecurity incidents and potential impacts.
- Extended downtime training and education.

Exercises

- Evolve exercises to include cybersecurity and downtime objectives.
- Integrate downtime exercising into regular maintenance windows.
- Start small and build over time.
- Workshop, TTX, Simulation, Full Scale Exercise

WORKSHOPS | EXERCISES | SIMULATIONS

MULTI-DISCIPLINARY

- Leverage Emergency Management partnerships.
- Identify opportunities for leadership and executive participation.
- Include departments in the planning process.

OBJECTIVE DRIVEN

- Define SMART objectives and used them to evaluate exercise deliverables.
- Identify a specific scope and anticipated outcomes.
- Outline participant expectations and responsibilities.

PROCESS IMPROVEMENT

- Request feedback from all participants and observers.
- Develop an After-Action Report / Improvement Plan.
- Utilize opportunities to drive adjustments and updates to process.

SUMMARY

- Cyber Security attacks in healthcare often result in extended downtimes and potential impacts to patient care.
- Current downtime and continuity plans rarely offer the necessary level of preparedness.
- It is imperative to develop a more resilient approach to extended downtime response.

QUESTIONS

Lisa Bisterfeldt

Program Manager, Cyber Resiliency

St. Luke’s Health System

bisterfl@slhs.org