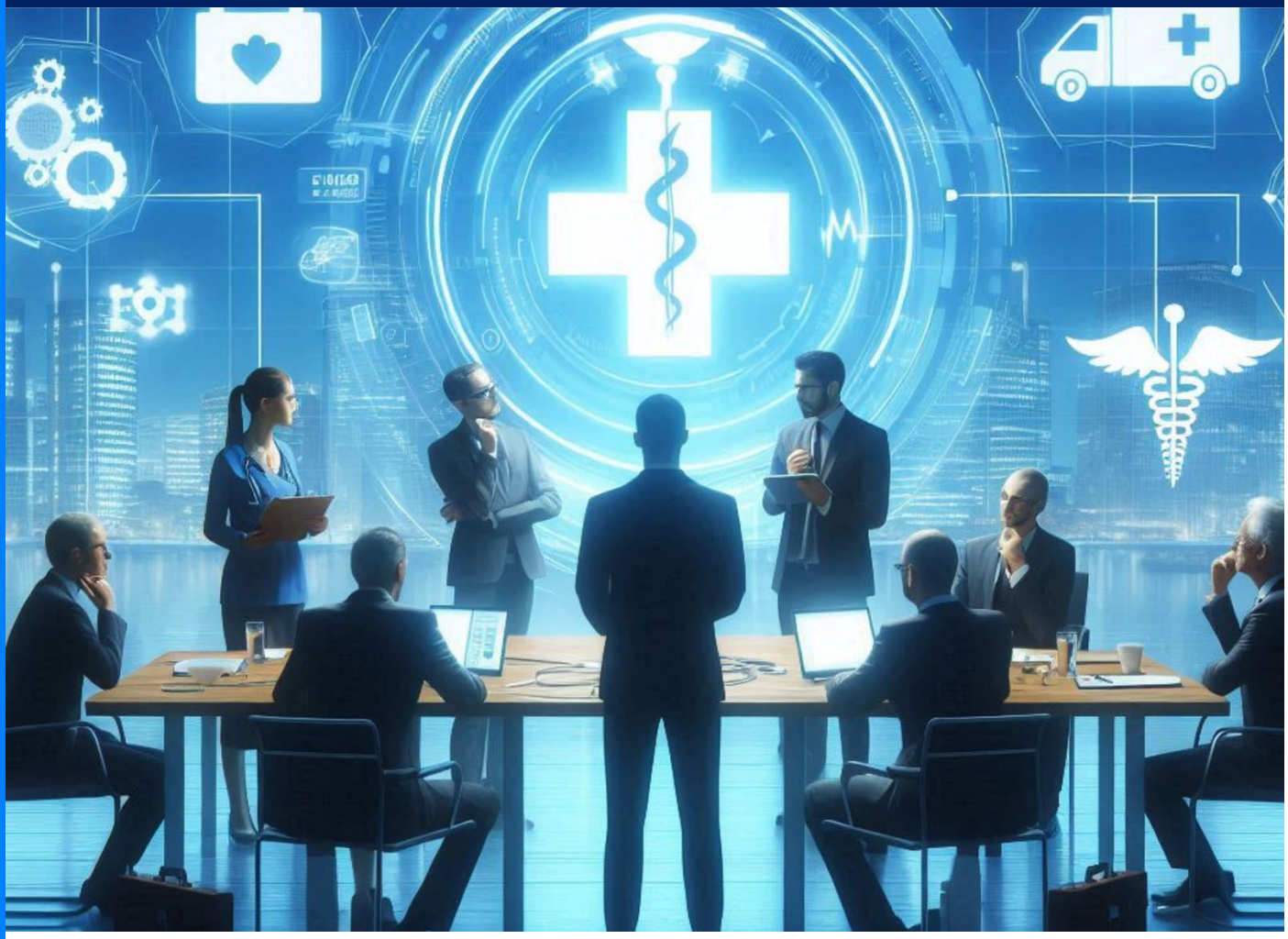
Health Sector Coordinating Council
Cybersecurity Working Group

Respond & Recover

HEALTH INDUSTRY CYBERSECURITY

From Panic to Plan: Executive Strategies for Handling Cybersecurity Incidents



OCTOBER 2024

Table of Contents

1. Introduction

Cybersecurity attacks against the healthcare sector are on the rise. In 2023, an average of 2 healthcare data breaches exposing more than 364,571 healthcare records on average were reported each day, with an average HIPAA fine of $1.5 million. The rate of ransomware attacks against healthcare organizations has reached a four-year high since 2021, impacting two-thirds of 400 healthcare organizations according to one estimate by Sophos. Accompanying this surge are higher recovery times and costs, with the mean cost of recovery in a healthcare ransomware attack at $2.57 million in 2024, double the 2021 cost. In 2024 alone, 60 reported ransomware attacks have resulted in class-action litigation, further imposing crippling costs on healthcare organizations. Many of these incidents are the result of attacks against business associates, third-party vendors and suppliers.

The impact of cyber-attacks on healthcare providers, payers, health IT, and medical products companies, whether direct or through business partners and solution providers, can be overwhelming: industry-wide delays in claim processing, research and intellectual property theft, postponed operations, unplanned overtime hours, inaccurate or incomplete patient data, and widespread destruction of blood donations due to mission critical systems being compromised.

And who must deal with the aftermath of these incidents? Consequences across a victim organization invariably involve executives responsible for legal, regulatory, operational, reputational, financial and clinical risk, and ultimately, patient safety.

The epidemic of cyber threats and incidents on the health sector highlights the need for healthcare executives not only to recognize the potential business consequences of cyberattacks but to understand and manage the executive role in directing and supporting incident response and continuity of operations.

Emergency management, business continuity, and disaster recovery plans are typically established to address natural disasters, physical safety events, pandemics, and technical outages. But the emerging threat of cybersecurity incidents warrants additional preparedness, as they present unique challenges that require specialized considerations. Preplanning establishes the framework for a swift cyber incident response, delineates contingency and continuity plans, and facilitates the quick resumption of services

This checklist aims to raise awareness about critical considerations for informed and swift executive decision-making during and after a cybersecurity incident. These considerations are categorized into Incident Response, Business Continuity, and Communication sections below. By familiarizing themselves with these strategic concerns in advance, healthcare executives can enhance their preparedness to ask the right questions and make effective decisions during a crisis.

2. About the Health Sector Coordinating Council Joint Cybersecurity Working Group

The Health Sector Coordinating Council (HSCC) Joint Cybersecurity Working Group (JCWG) is a government-recognized critical infrastructure industry council of more than 450 healthcare providers, pharmaceutical and medical technology companies, payers, health IT and government entities partnering 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. See https://HealthSectorCouncil.org.

3. Executive Checklist for Cyber Incident Response

Incident Response

The response to a cybersecurity event can be complex, requiring a comprehensive array of actions.

The foundation of an effective incident response is the identification of a team and development of a plan that is exercised to ensure timely activation. Key advance preparedness elements for a streamlined response include:

- Collaboration with risk management and legal counsel to consider an optimal cyber insurance policy, balancing coverage levels, premium costs, and risk management requirements.
- Engaging in proactive discussions with executive leaders, board members, and legal counsel regarding extortion policies and the authority to negotiate demands or payments.
- Identifying who within the organization has the authority to take all technology systems offline. This is typically a time-sensitive decision that may be necessary to limit the spread of an attack yet needs to be balanced against clinical needs.
- Contracting with cyber security response firms prior to an incident to foster partnerships, expedite planning and minimize response costs.
- Establishing protocols for sharing information with internal and external partners, including patients, healthcare organizations, vendors, staff, and the public.
- Mapping and prioritizing criticality of essential services with a recommended restoration sequence during an extended downtime event.

Business Continuity

Healthcare relies heavily on technology to ensure patient safety and maintain efficient business operations. Even a brief technology outage can pose significant patient safety risks. The repercussions of a cybersecurity incident extend beyond the technical environment, often leading to prolonged operational downtimes and disruptions, which could last multiple weeks to months. Typically, downtime and continuity plans are limited in scope and primarily support short, planned outages.

To develop robust processes and resources for sustaining extended downtime events, consider the following continuity considerations:

- How will operations continue if the technical network is taken offline, and technology is unavailable?
- Which services will be suspended to manage downtime, and who has the authority to suspend services within the facility?
- If a system goes down, do you understand how it affects other systems and business processes?
- Is there a comprehensive list of technical, clinical, and operational vendors with up-to-date contact information?

- Do all patient and operational areas have procedures in place to support an extended downtime event and are they reviewed regularly?
- What federal, state and local, and tribal regulatory reporting notifications are required, and who is responsible for making these notifications?
- What will be the impact on hospital billing, revenue cycle, cash flow, and payroll operations during an extended downtime event?
- How will clinical trials and research be managed in relation to grant funding and FDA requirements?
- What are the potential implications for the supply chain during an extended downtime event?
- How will you secure your facility if access control systems are impacted or unavailable
- How will staff communicate if traditional communications mechanisms such as phone and email are unavailable or untrusted?

Communications

Effective communication is crucial during a cybersecurity incident. It must be clear, concise, factual, and timely. Incident management relies on collaboration and understanding the organization's capabilities and response plans. Pre-incident discussions can enhance these plans and protect the organization, staff, and community from cybersecurity attacks and downtime.

Key considerations for communication during a cybersecurity incident include:

- Before an incident occurs, establish a crisis communication plan that outlines the information the organization is prepared to share during a cybersecurity event. The communication plan should include tailored templates for various audiences, including:
  - Board of Directors
  - Patients and Customers
  - Vendors and Contractors
  - Staff and Providers
  - Partner healthcare agencies and cybersecurity collaboratives.
- Be aware that internal communications may be inadvertently shared with external media outlets, partners, regulators, social media channels, or other entities. Establish clear policies for the internal chain of command regarding external communications.
- Be aware that if law enforcement is engaged as part of your forensics and incident response, law enforcement may circumscribe external communications about the incident “due to an ongoing investigation.” This muting of some information to the public can introduce reputational and misinformation risk.
- Provide status updates, specific instructions, and foster a culture of teamwork, empowering staff to continue performing their roles effectively.
- Alert partner organizations to immediate risks posed by the incident.
- Consider sharing information about identified vulnerabilities or indicators of compromise with cyber security peer networks or information sharing organization to help prevent similar attacks.

4. Additional Resources

Effective cybersecurity responses demand the collaboration of Emergency Management, Information Technology, Clinical, Operational, and Cybersecurity programs to manage the interdependencies and tactical nuances arising from a cybersecurity incident. This Checklist address those collaborative imperatives and supplements leading practices published by HSCC in other incident response and operational continuity resources, including (links embedded):

Operational Continuity Cyber Incident (OCCI)

Flexible checklist tool aligned with the Hospital Incident Command System framework to guide response actions for the first operational period of a cyber security attack resulting in a widespread downtime event. Organizations can adapt the suggested structures and tasks based on their size, resources, complexity, and capabilities.

Coordinated Healthcare Incident Response Plan (CHIRP)

Technical cybersecurity incident response template designed for health systems, hospitals, and clinics, including recommendations and guidance for responding to the incident while facilitating collaboration between hospital and leadership teams to ensure a coordinated and effective response.

Cyber Security for the Clinician Video Training Series

An eight-part video series tailored for clinicians to boost cybersecurity awareness, identify risks, and learn how to mitigate cyber threats. Participants can earn one CME/CEU credit hour, and the series may help fulfill documentation requirements for the CMS Emergency Preparedness Rule, the National Fire Protection Association, and The Joint Commission.

For other leading practices in healthcare cybersecurity, visit https://healthsectorcouncil.org/hscc-publications/.

***

Feedback

To provide feedback about this document, please reference the document name and share your comments to Feedback@HealthSectorCouncil.org

5. Acknowledgments

The HSCC Cybersecurity Working Group wishes to thank the Incident Response and Business Continuity (IRBC) Task Group and, in particular its task group leaders for producing this third in a series of incident response resources for the benefit of the security and resiliency of the health sector. Their tireless efforts and dedication to the imperative that Cyber Safety is Patient Safety serves as a compass for how we all pull together in shared responsibility against cyber threats to the health sector. To beat one of us, the adversaries have to beat all of us.

Incident Response Business Continuity Task Group

Co-Leads

Lisa Bisterfeldt, St. Luke's Health System

Mike Caudill, Duke Health

Nate Couture, University of Vermont Health

Garrett Hagood, Coastal Bend Regional Advisory Council

Darrell Hall, HHS Health Sector Cybersecurity Coordination Center (HC3)

Members (affiliations at time of enrollment)

Troy Adams, HHS HC3

Michael Alicea, Business Intelligence Group

Craig Allen, Intermountain Healthcare

Ana Sofia Arevalo, UCSD Medical Center

Christopher Ashby, Fresenius Medical Care

Laura Baker, Cyber Wyoming

Erik Berg, Siemens Healthineers

Jay Bhat, Franciscan Health

Michael Bjorklund, Select Health

Brian Blackburn, Compassus

Gerry Blass, Comply Assistant

Curtis Blythe, Abbott

Scott Bolak, University of Michigan

Jeff Bontsas, Ascension

Reese Borel, Cardinal Health

Stacey Bradley, Health Resource Group

Jeanie Brand, FDA

Julie Breaux, Rush University Medical Center

Eric Campbell, Friend Health

Robert Cantu, INOVA Health System

Stephen Carroll, Becton Dickinson

James Case, Baptist Health NE Florida

Michael Challenger, New York-Presbyterian Hospital

Uma Chandrashekhar, Alcon

Hazel Chappell, ishca health

Penny Chase, MITRE

Bonnie Chen, Hospital Sisters Health System

Matt Christensen, Intermountain Healthcare

Shawn Clark, Cleveland Clinic

Jessica Clayton, Blue Cross Blue Shield of Alabama

Bennie Cleveland, Beebe Healthcare

Adam Cole, LifeOmic

Stephen Collins, Impact Advisors, LLC

Doug Copley, AtlantiCare Health System

Sara Coverstone, Northern Arizona Healthcare

Brindusa Curcaneanu, NeuroPace

Philip Curran, Cooper University Healthcare

Tyler Curry, Health-ISAC

Megan Curtis, Intermountain Healthcare

Christian Dameff, UCSD Medical Center

Tom Davis, Thermo Fisher Scientific

Aaron de Montmorency, Elevate Health

Erik Decker, Intermountain Healthcare

Drex DeFord, This Week Health

Scott Didion, SSM Health

Jack Dimpsey III, Oklahoma State Department of Health

Frank Domizio, Mom's Meals

Sharee Dorsey, Cleveland Clinic

Julia Doveikis, Smith + Nephew

Scott Draper, UnityPoint Health

John Eby, VSP

Jake Edwards, UVA Health

Stacy Estrada, Montage Health

Joshua Fishel, Wellspan Health

Justin Formosa, Women's Care Florida

Zack Gable, Geisinger

Fabricio Gamboa, Southern Illinois Healthcare

Greg Garneau, Hospital Sisters Health System

Luis Gatti, Johnson & Johnson

Brian Gilbaugh, Duke Health

Ruth Gittens, Becton Dickinson

Brittany Glover, Baptist Healthcare Systems Inc. KY & IN

Ben Goodman, 4A Security & Compliance

Ryan Gott, Adaptive Biotech

Chris Graham, Presbyterian Healthcare Services

Damian Grant, Amgen Inc.

Les Gray, Abbott

Tina Greene, Cooperative Exchange

Andrea Greene-Horace, HHS

Kimberly Grotz, Wills Memorial Hospital

Liviu Groza, Cape Cod Healthcare

Ajay Gupta, Cencora

Hannah Haakana, St. Luke's Health System

Karen Habercoss, University of Chicago Medicine and Biological Sciences

Mike Hamel, Hoag Health

Jacob Hammersmith, Billings Clinic

Gary Haney, Ballad Health

Patrick Headley, UVA Health

Jon Helgason, Sodexo

Shawna Hofer, St. Luke's Health System

Kim Hogstad, Sanford Health

Harwell (Navar) Holmes Jr., Campbell County Health

Zack Hornberger, Advanced Medical Technology Association

Stephen Hughes, American Hospital Association

Kathy Hughes, Northwell Health

Monique Imroth, UCSD Medical Center

Jim Jacobson, Siemens Healthineers

Mark Jarrett, Northwell Health

John Jeffries, University of Tennessee Medical Center

Ishan Khadka, Cape Cod Healthcare

Jim Kinsman, McKesson

Scott Lagger, University of Illinois (Chicago) Hospital

Dennis Leber, Ph.D.,Honest Medical Group

Rick LeMay, First Health Advisory

Alex Lichtenstein, UCLA Medical Center

Chris Logan, Blue Cross Blue Shield of Rhode Island

Robert Maclay, Stanford Medicine Children's Health

Om Mahida, MedCrypt

Mary Massey, California Hospital Association

Jackie Mattingly, Clearwater Security

John Matusiak, Takeda

Brian Mazanec, HHS

George McCaffrey, Penn State Health

Brian McCormack, Intermountain Healthcare

Brady Miller, Methodist Le Bonheur Healthcare

John Miller, University of Louisville Health

Jason Miracle, Cardinal Health

Ravi Monga, St. Luke's Health System

Deb Muro, El Camino Health

Cherrie Murphy, Southwest Regional Health Systems

Tomislav Mustac, Mount Sinai Health System

Joshua Myers, Blue Cross Blue Shield of Louisiana

Leslie O'Connor, Labcorp

Teddy Onyenaucheya, Becton Dickinson

Nirav Panchal, Baxter Healthcare Corporation

Mitchell Parker, Indiana University Health

Reuven Pasternak, DHS CISA

Kate Pierce, Fortified Health Security

David Pittman, UT Medical Center

Ryan Potts, Thermo Fisher Scientific

Andy Price, St. Claire HealthCare

Amy Puglia, Duke Health

Sethu Raman, Organon

TJ Ramsey, Fortified Health Security

Chris Rathermel, Spero Health

Pyreddy Reddy, North Carolina Department of Health and Human Services (NCDHHS)

Janice Reese, NetworkPDF Inc.

Phillip Rizzo, Shirley Ryan AbilityLab

Keith Roberts, Abbott

Renee Rodriguez, Austin Radiological Association

Jim Roeder, Lakewood Health System

Emily Rugo, Northern Arizona Healthcare

Sonia Sadana, PNC Bank

Michael Sanders, Lawrence County Memorial Hospital

Samina Sanwarwala, CommonSpirit Health

Andrew Sargent, Werfen

Blake Scott, Coconino County Health and Human Services

Jennifer Sears, The Coordinating Center

Philip Shen, Memorial Sloan Kettering Cancer Center

Eirene Shipkowitz-Smith, MedSec

Devin Shirley, Arkansas Blue Cross Blue Shield

Michael Shrader, Wellspan Health

Edmund Siy, Hunterdon Health

Skip Skivington, Kaiser Permanente

Arnicia Smith, American Red Cross

Dallas Smith, Burn and Reconstructive Centers of America

Allison Snyder, Johnson & Johnson

Thomas Stidham, Texas Health Resources

Heath Stockton, Booz Allen Hamilton

Samuel Stone, HHS

Tim Streit, Roche Diagnostics

Joe Susai, Washington University School of Medicine in St Louis

Christopher Talcott, OSF Healthcare

Joshua Taylor, Viatris

Russell Teague, Fortified Health Security

John Thomas, SSM Health

Sara Torres, University of Chicago Medicine

Scott Trevino, TRIMEDX

Thomas Tropasso, Penn State Health

Priyanka Upendra, Asimily

Rachel Vaichus, Thermo Fisher Scientific

Preeti Vaidya-Gupte, Walgreens Boots Alliance

Jamie Vance, Cardinal Health

Ramya Varadharajan, Indiana University Health

Leon Vinci, Health Promotion Consultants

Jeremy Walton, AbbVie Pharmaceutical

Jake Wardon, Synchron, Inc.

Alastair Webb, Inari Medical

Kristy Westphal, HealthEquity

Jessica Wilkerson, FDA

Sherry Wilson, Cooperative Exchange

Joe Wivoda, HIPAATrek

Chris Wolfe, Main Line Health

Dee Young, UNC Health

Margie Zuk, MITRE

Raymie Zychowski, Health Care Services Corporation