Health Sector Coordinating Council
Cybersecurity Working Group

Manage Risks | Monitor Threats | Respond & Recover

Health Industry Cybersecurity -

Tactical Crisis Response (HIC-TCR)

AUGUST 2023

Reprint of 2020 Edition

Table of Contents

Introduction

In light of annual hurricane season and the necessary emergency procedures necessary for preparation, operational continuity and recovery, this reprint of the May 2020 edition of the Health Industry Cybersecurity Tactical Crisis Response guide, developed jointly with the Health Information Sharing and Analysis Center (Health-ISAC), is a timely reminder for all healthcare organizations to ensure their crisis response plans are up to date and trained.

Within healthcare, a crisis can occur at any moment inside any organization. It could be a regional hazard, specific to a healthcare organization, or related to a national crisis (such as a pandemic). One thing is certain, when a crisis occurs healthcare organizations need to be ready to stand up emergency operations, such as the Hospital Incident Command System (HICS).

Depending on the crisis, the level of cybersecurity threat against an organization might vary. Some of these events occur so quickly there might not be an opportunity for threat actors to take advantage. In other cases, such as during a pandemic, the period of exposure widens significantly. In either case, preparation is the key.

Unfortunately, healthcare organizations might be at different levels of preparation for such an event or have minimal resources available to adequately prepare. When the crisis hits, organizations might be left scrambling while standing up an unplanned response.

Therein lies the value of this document. During a crisis, organizations need a tactical response for managing the cybersecurity threat that can occur. This document is constructed by industry and government experts to help guide through response activities. Smaller organizations can leverage this document as a list of activities to consider. Larger organizations can leverage this document as a sanity check for existing plans. In either case the level of risk and exposure to any organization is specific. The activities listed here are suggestions to help with a practical and tactical response and are not intended to account for any given organizational incident response plan.

This document is organized into four suggested areas of focus:

1. Education and Outreach, considerations for organizational engagement
2. Enhance Prevention Techniques, considerations for preventing attacks
3. Enhance Detection and Response Techniques, considerations for discovering and responding to attacks
4. Take Care of the Team, considerations for assisting your team

After reviewing these suggestions, the document also suggests a mechanism for self-assessment and provides guidance on how to leverage these suggestions based upon risk.

Lastly, this document provides a list of resources available to the industry from key partners, such as H-ISAC, the U.S. Department of Health and Human Services, the U.S Department of Homeland Security, as well as the Health Sector Coordinating Council.

Acknowledgements

While applicable to all emergency management situations, this guide was created during the national COVID-19 pandemic in 2020, while healthcare organizations quickly transitioned to care for patients stricken by the SARS-

CoV-2 virus, implemented telemedicine visits and moved a large portion of their workforce home in order to establish social distancing parameters to slow the spread of the disease. The creation of this guide could not have been accomplished without the dedication of the below hardworking individuals within our healthcare industry.

In the middle of this national crisis, these individuals came together within the Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG) and the Health Information Sharing and Analysis Center (H-ISAC) to establish this guide to help others manage through these unprecedented times. It is with greatest gratitude we thank the individuals below for going above and beyond. ***This list includes individuals and their organizational affiliations in 2020, which in some cases are no longer current.***

Mike Gross
Cleveland Clinic

Craig Barber
Duke Health

Mike Caudill
Duke Health

Tony Enriquez
CISA

Jon Crosson
H-ISAC

Ed Brennan
H-ISAC

Denise Anderson (Co-Lead)
H-ISAC

Greg Garcia
HSCC CWG

Omar Tisza
HSCC CWG

Anna Verrichia
Merck & Co, Inc

Martin Fisher
Northside Hospital

Kim Sassaman
Presbyterian Healthcare Services

Lenny Levy
Security Cubed Consulting

Jamie Piece
Sentara

Erik Decker (Co-Lead)
UChicago Medicine

Ali Kapucu
UChicago Medicine

Framing the Problem

Criminals love to take advantage of a crisis. During the COVID-19 crisis, threat actors leveraged the pandemic to deploy phishing, malware, remote access, teleworking and domain attacks[1]. The efficacy of these attacks was

1 COVID-19 Exploited by Malicious Cyber Actors https://www.us-cert.gov/ncas/alerts/aa20-099a

bolstered by the rapid change the health industry made in order to care for sick patients, deploy remote diagnostic and therapeutic treatments and shift a large portion of its workforce to work from home.

While the COVID-19 pandemic has fundamentally changed the landscape, it is not unusual to make sudden and drastic changes to the technology platforms that support an organization's crisis management activities. These changes can introduce new vulnerabilities and new attack vectors. Coupled with an increase in threat activity, organizations can be left with a perfect-storm style scenario that gives an advantage to the threat actors.

During a crisis, the importance of an organization's cybersecurity posture is even more evident; for each gain delivered by automation, interoperability, and data analytics, the vulnerability from malicious cyber-attacks increases as well. To thwart these attacks before they occur, it is essential for health care organizations to establish, implement, and maintain current and effective cybersecurity practices.

Tactical Crisis Management Techniques and Practices

This document outlines four groups of techniques, practices, and activities that can be leveraged during a crisis. This is not intended to be an exhaustive list of action, nor is it intended to replace an overarching incident response plan. The actions below are important considerations, whether there is no incident response plan, or a highly mature plan that is to be further developed.

- Education and Outreach
- Enhance Prevention Techniques
- Enhance Detection and Response
- Take Care of the Team

1. Education and Outreach

While much of the success of the cybersecurity response to a crisis is driven by technical controls, the value of effective organizational education and outreach as a force multiplier cannot be underestimated. Communication plans that are well thought out and properly executed will reduce confusion, improve response times, and maximize the effectiveness of the overall cybersecurity plan. It is important to be both transparent and timely in communications to stakeholders.

Communication Plans

In order to effectively communicate with stakeholders, a plan that defines the various methods and channels to deliver messages must be in place. Audiences will differ depending upon the nature of the incident; organizational, clinical IT leadership, and vendor support should be included. Consider the following components of a communication strategy:

Organizational Leadership Communication Plan

Target Audience: Leadership (administrative, operational, clinical)

Channels: Hospital Incident Command System (HICS), Emergency Management, Leadership Meetings, Town Halls, Email

Plan Elements:

- Ensure understanding of ongoing actions to validate and enhance cyber posture and potential adverse impacts to operations
- Ensure the cyber communication plan is integrated and supportive of the overall organizational communications plan such as HICS
- Ensure communications are on a stated cadence and regular format

IT Leadership Communication Plan

Target Audience: IT Leadership

Channels: Leadership Meetings, Change Management, Daily Standups, Email

Plan Elements:

- Technology changes occurring, risks associated with changes, and cyber threats
- Ensure technology users know to report to the cybersecurity team any unexpected outages or issues with assets and to notify appropriate leaders of any changes being made to the environment
- Consider Government Emergency Telecommunications System (GETS) and Wireless Priority Service (WPS) for qualified users

Clinical Leadership Communication Plan

Target Audience: Clinical Leadership

Channels: HICS/Emergency Management, Clinical Standups, Clinical Operations Meetings, Email

Plan Elements:

- Ensure understanding of any changes that would impact delivery of care or expected workflows (such as telemedicine, EMR workflow changes, remote access changes, etc.)
- • Provide points-of-contact for clinical leaders to engage with cyber leadership to discuss any unexpected modifications to cybersecurity controls

All Users Communication Plan

Target Audience: All Employees, Contractors, Consultants, Volunteers, Locums, etc.

Channels: Newsletters, Intranet, Bulletin Boards, Video, Daily Standups (through Leadership), Email, Mass Notification Systems (for emergencies)

Plan Elements:

- Creation and distribution of a tip sheet providing latest guidance, updates, and information on a regular cadence that helps improve dissemination of critical information across an organization
- Coordinate existing emergency management communications and stay consistent with established practices outlined by Marketing, Public Affairs and Legal

- Consider centering communications around known threats (phishing, malware, etc.) and provide simple, actionable and effective guidance that contains, at least:
    - How to identify threats (spearphishing, business email compromise, etc.)
    - Where to report threats (cybersecurity teams)
    - What to do if a victim ("see something say something")
    - Reinforce non-retaliation
    - Expectations around confidentiality of internal business information, which include clear media protocols
- Communicate best practices that are actionable by all users. For example:
    - Securing home wireless network (Wi-Fi) if remote working
    - Protecting company information
    - Securing devices including BYOD
- For Mass Notification Systems (MNS):
    - Gather additional communication touchpoints for staff (personal phone trees, personal email, etc.) in the event of corporate system inoperability
    - Ensure only authorized individuals can approve and distribute communications via MNS channels
    - Ensure relevant processes and procedures modified or static are communicated

External Communication Plan

Target Audience: Media outlets, Vendors, Patients

Channels: Public Affairs and Marketing / Communications Professionals, Social Media and Websites as determined by the organization's needs.

Plan Elements:

- Verify all media interaction protocols with Legal and Communications departments, ensure consistency with emergency management communications plans
- For patient communications, engage Privacy Programs & Legal (if related to privacy breaches), Call Centers/ Scheduling departments, patient success professionals, etc.
- For third party vendors, engage with Supply Chain department stakeholders who own relationships with vendors; if related to a security incident, ensure protected communications by leveraging Legal and Privacy Programs
- Make every effort to participate in and share incident indicators and lessons learned with communities of sharing. Sharing communities are valuable sources for learning information and response strategies

Policy and Procedure Review

In the event of a crisis policies might be adjusted, relaxed, or have exceptions. Consider that exceptional circumstances might pressure existing policy structure. Though it is important for cybersecurity teams to be flexible with the organization they also, at a minimum, must track these exceptions during any crisis to guide the

organization back to normalcy once the crisis is over and inform continuous improvement processes. Consider these elements:

- Collaborate with existing emergency management leadership channels, (e.g., EOC, HICS) as well as Legal, Compliance, IT and other stakeholders to build strategies related to policies that may need to be adjusted, amended or relaxed
- Consider regulatory obligations when relaxing any policies; even if the regulator has relaxed enforcement actions during any crisis, enforcement will return upon recovery
- Review, update, and validate all relevant policies including Remote Work, Access Control protocols, Acceptable Use, Password & Multifactor, and Identity Governance
- Consider policies and procedures that enable collaboration with external parties / agencies and determine if any operational changes are needed
- Document all changed security assessments and exceptions so that, upon normalcy, the organization can revert if needed
- Allow for development and deployment of websites, applications, file sharing, etc., that may be temporary or permanent depending on the specific situation; track these new technologies for possible improvements and security assessments
- Consider augmentation capabilities of IT / cybersecurity staff in order to 'scale up'
- Review, update, and validate policies related to adding temporary, locums, or other volunteers into the organization
- Review, update, and validate policies on physical security of assets and coordinate with appropriate teams on possible required exceptions or mitigating controls
- Assess procedures to quickly and securely activate or deactivate organization locations to support clinical / operational efforts

2. Enhance Prevention Techniques

Prevention of cyber-attack impacts is the goal. Many organizations already have a suite of prevention capabilities in place, such as access control, firewalls, intrusion prevention, spam prevention and so on. In this section we outline three practices to consider reviewing:

- Limit Potential Attack Surface
- Bolster Remote Access
- Leverage Threat Intelligence Feeds

Limit Potential Attack Surface

Cybersecurity teams must defend all entry points into an organization's assets and data while the threat actor only needs to find one. Reducing the attack surface as much as possible improves resiliency. The following techniques can assist with that goal.

Vulnerability Management

While attackers continually scan the Internet for vulnerable systems, during a crisis they may seek out zeroday or previously unknown vulnerabilities. To reduce the likelihood of vulnerabilities being exploited, consider these elements:

- Conduct a review of ingress / egress points and Internet facing Applications and Servers for critical vulnerabilities
- Validate externally and internally exposed IT assets using available scan and survey tools
- Repeat validation as often as possible to ensure no vulnerable assets are exposed
- If operationally possible, remove from service any vulnerable externally facing assets that cannot be patched
- Leverage threat intelligence feeds and monitor for attacks against vulnerable assets

Accelerate Patching

When vulnerabilities are found, ensure all externally facing assets are fully patched. Consider a weekly security touch base with key application owners and the security operations team to ensure critical patching is occurring. Where possible, next generation firewall capabilities including Cloud Access Security Broker, drive-by download protection, malware sandboxing, and Intrusion Detection and Prevention System (IDS/IPS) capabilities should be enabled.

Medical Devices

Medical devices and Internet of Things (IoT) devices might pose risk due to patching difficulties. Consider the following:

- Review vulnerabilities of networked medical devices and deploy validated critical patches
- Identify all vendor remote access channels into the network environment using a vendor managed remote access technology
- Limit remote access into the environment from these identified channels

Vendors

Besides vendors managing medical / IoT devices, there may be other third parties that have network access. Consider the following:

- Identify any third-party connections that are not needed, take a “close the ports” approach to minimize ingress/egress
- Perform periodic access reviews of vendor accounts and remove accounts that are no longer needed
- Consider suspending federated connections, if any

Endpoint

Within a given crisis, employees may operate remotely. As such consideration should be made that devices normally operated within a known facility might end up moving outside of the environment. Consider the following:

- Ensure asset management systems can connect to and manage and patch devices while “off-network”
- Ensure devices are encrypted, especially if they leave the physical security of the healthcare environment

- Review and deploy anti-virus technologies
- Leverage a mobile device management (MDM) or mobile application management (MAM) solution to ensure mobile devices are adequately protected

Bolster Remote Access

Remote workforce operations increase in any crisis. Existing remote access methodologies might become the primary channel for a large portion of the workforce in continuation of duties. The following techniques can assist with securing remote access.

Deploy Multi-Factor Authentication

To reduce the likelihood of stolen / guessed credentials being used for unauthorized access, leverage multi-factor authentication to limit access to organizational resources. Consider deploying multi-factor authentication for the following technologies:

- Virtual Private Network (VPN)
- Remote Desktop Protocol (RDP)
- Citrix
- Virtual Desktop Infrastructure
- Referring provider EMR portals
- Cloud based solutions, such as Office 365, G-Suite, AWS, Azure, HR systems, Payroll

To get the best coverage possible for Multi-Factor Authentication (MFA), integrate MFA with your Single SignOn (SSO) system and connect SSO to your cloud-based solutions.

General Authentication

Some solutions might still require single-factor authentication access. These types of systems are more susceptible to phishing and credential attacks and should ideally be restricted from direct Internet access. Consider applying the following methods:

- Limit access to remote single-factor authentication channels, especially if these are vendor managed channels and not part of your enterprise remote access suite
- Limit the amount of shared accounts, especially for vendors; ensure users are granted individual user accounts
- If feasible, consider implementing geo-authentication blocks from countries currently considered high threat by the Cybersecurity and Infrastructure Security Agency (CISA) while understanding unintended consequences of geo-blocking; countries considered high threat can be found under “Current Cyber Threats” on the CISA cybersecurity page[2]
- Ensure all single factor authentication options follow NIST password guidance and lock after incorrect credentials are entered multiple times

[2] CISA: Cybersecurity https://www.cisa.gov/cybersecurity

- For Microsoft O365 environments explicitly block legacy authentication with conditional access to ensure MFA is required for all connections[3]

Leverage Threat Intelligence Feeds

During a crisis, the threat environment can change quickly and may require quick action. Intelligence rapidly acted upon increases the ability to prevent and respond effectively. Machine to Machine (M2M) threat intelligence combines with security solutions already in use and may help prioritize and refine threats and alerts. The goal with threat intelligence will be to enable automated blocking of known malicious threat actors.

For a comprehensive guide on establishing and consuming information sharing intelligence, consider reviewing the Health Industry Cybersecurity Information Sharing Best Practices (HIC-ISBP) guide[4]

Setup

Where possible, automate the consumption of information via Structured Threat Information eXpression (STIX) / Trusted Automated eXchange of Indicator Information (TAXII). Below are some options for appropriate tools:

- Organizations that do not have a TAXII capability can use open-source TAXII clients available on GitHub (Cabby[5], Minemeld[6])
- Some next-generation firewalls enable threat feed consumption
- Some Security Information and Event Management (SIEM) systems enable threat feed consumption
- Some Security Orchestration, Automation, and Response (SOAR) systems support threat feed consumptions

Organizations that don't have M2M capability internally might work with threat intelligence or third-party service providers to ensure they are incorporating threat intelligence feed sources.

Integration with firewall and/or proxy systems to enable automated blocking of known threats is performed once the threat feed system has been set up.

Threat Feed Sources

Numerous sources exist that will enable consumption of feed intelligence. For feed sources that support STIX/ TAXII integration, the ability to automatically feed the list into prevention systems (such as firewalls or proxies) exists. Below is a list of feed sources:

---

[3] How to: Block legacy authentication to Azure AD with Condition Access https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication
[4] Health Industry Cybersecurity Information Sharing Best Practices https://healthsectorcouncil.org/info-sharing-guide/
[5] Cabby https://www.eclecticiq.com/open-source/cabby
[6] Minemeld https://github.com/PaloAltoNetworks/minemeld/wiki

Source	Automated Feeds	Overview
H-ISAC	Yes	H-ISAC is a global, non-profit, member-driven organization offering healthcare stakeholders a trusted community and forum for coordinating, collaborating and sharing cyber threat intelligence and best practices with each other. H-ISAC is a trusted community of critical infrastructure owners and operators within the Healthcare and Public Health Sector. Automated sharing may include connections through multiple internal and external sources, including, but not limited to, Celerium's Soltra Edge, Anomali ThreatStream, TruStar, CISA AIS and CISCP Programs, Perch Security, other ISACs, International CERTs, along with numerous managed service providers (MSPs). Data is available in various formats including, but not limited too, STIX/TAXII, JSON, XML, CSV, and MISP protocols. Threat data is also shared manually through email, chat, website, and other communication platforms.[7]
CISA AIS	Yes	The Cybersecurity and Infrastructure Security Agency's (CISA) free Automated Indicator Sharing (AIS) capability enables the exchange of cyber threat indicators between the Federal Government and the private sector at machine speed. Threat indicators are pieces of information like malicious IP addresses, FQDN, URL and the sender address of phishing emails.[8] CISA uses STIX/TAXII for the connection. It requires a PKI certificate from a commercial provider, whitelisting your IP address, and sign an Interconnection Security Agreement. You can also share indicators with CISA through a participating ISAC or ISAO.
Infragard	No	The FBI's InfraGard Portal serves as a clearinghouse for the public and private sectors to share information to protect America's critical infrastructure. The site offers Cyber Crimes and Cyber Fugitives links that contain information on the most recent attacks and potential threats being tracked by the FBI.[9]
SANS Internet Storm Center	No	The ISC relies on an all-volunteer effort to detect problems, analyze the threat, and disseminate both technical as well as procedural information to the general public. Thousands of sensors that work with most firewalls, intrusion detection systems, home broadband devices, and nearly all operating systems are constantly collecting information about unwanted traffic arriving from the Internet. These devices feed the DShield database where human volunteers as well as machines pour through the data looking for abnormal trends and behavior. The resulting analysis is posted to the

[7] H-ISAC https://h-isac.org/
[8] Automated Indicator Sharing (AIS) https://www.us-cert.gov/ais
[9] InfraGard https://www.infragard.org/Application/Account/Login

		ISC's main web page where it can be automatically retrieved by simple scripts or can be viewed in near real time by any Internet user.[10]
Spamhaus	No	The Spamhaus Project is an international nonprofit organization that tracks spam and related cyber threats such as phishing, malware and botnets, provides realtime actionable and highly accurate threat intelligence to the Internet's major networks, corporations and security vendors, and works with law enforcement agencies to identify and pursue spam and malware sources worldwide.[11]

The above list is just a subset of possible options available for consuming threat intelligence information. A more comprehensive matrix of information sharing organizations can be found within the Health Industry Cybersecurity Matrix of Information Sharing Organizations (HIC-MISO)[12]

Establishing Confidence Levels

Threat intelligence comes from a variety of sources from both curated and community sources. Consequently, it may not be applicable to a given organization or completely accurate. When consuming information and indicators that are received from established threat intelligence feeds, consider the source and whether it is trusted or reliable before using the information in mitigation strategies.

Prior to applying threat intelligence to the environment, the confidence level should be determined (e.g., low, medium, and high). The confidence level can change over time based on new data, trust, and organizational risk thresholds. Consider these steps:

- Add context to the intelligence received (the source and details)
- Classify the intelligence based on the indicator
- Validate the quality of the information
- Confirm the confidence level of integrated feed sources (low, medium, high)

Once the confidence level is determined, organizations should act accordingly. For high confidence threats, consider the following:

- Leverage security tools (e.g., firewall, SIEM) to automate blocking and alerting
- Update SOAR solutions, to automatically implement countermeasures for collected intelligence
- Solutions should be able to update firewall rules, email rules, DNS, and other such devices which can quickly be modified to address threats. For known malicious sites or newly created sites named after the

[10] Internet Storm Center: Threat Feeds https://isc.sans.edu/threatfeed.html
[11] Spamhaus https://www.spamhaus.org/
[12] Health Industry Cybersecurity – Matrix of Information Sharing Organizations (HIC-MISO) https://healthsectorcouncil.org/hic-miso/

crisis (such as COVID19 during the 2020 pandemic) consider blocking by default and allowing if needed for a valid business reason. Similarly, block uncategorized URLs to limit access to newly created sites used for phishing or distributing malicious software links / software

For low and medium confidence threats, consider the following:

- Evaluate IOC 'hits' with your SIEM, firewall, proxies, etc, to determine level of concern
- Consider using these 'hits' as pivot points for further threat hunting activities

Finally, many attacks have a human component (e.g., phishing). Share relevant intelligence with end users and senior leadership regarding prevention, mitigation, and response.

3. Enhance Detection & Response

Not all attacks are preventable. It is therefore critical to have mechanisms to detect successful attacks and respond quickly. This might involve establishing new detection schemes in the environment as well as bolstering an existing incident response team. During an incident, organizations need to know what to do and who to call. Responding teams need to have tools and capabilities prior to the occurrence of an incident or at least the ability to gain those capabilities immediately on demand. The authority to direct the actions of others who may need to be involved is important for command of the crisis.

Enhance Detection Capabilities

To monitor for malicious access, there must be visibility in the form of logs. Consider ensuring the following consumed log sources into a centralized log repository or SIEM:

- Remote Access Logs (VPN, Citrix, VDI, RDP, etc.)
- Firewall Logs
- Multi-Factor Authentication Logs
- Active Directory / LDAP / Central Authentication Systems
- Server Logs
- RADIUS logs
- Network Access Control Logs

Once log sources have been established, detection capabilities and alerts within your SIEM in the event of a crisis are established.

- Monitor remote access login attempts, looking for brute force attacks, password spraying attacks (checking multiple user accounts with a single password from a few IP addresses), numerous logins to multiple accounts from the same source IP, etc.
- Identify accounts that passed username / password authentication, but failed multi-factor authentication multiple times
- Check the configuration of remote devices connecting into remote access systems, looking for encryption, A/V, OS patch levels, and approved applications

- Monitor Multi-Factor Authentications. Review MFA authentications to look for anomalous activity which could be indicated by login failures, geo locations, and login times
- Establish and monitor network traffic baselines. Establishing security objectives will allow you to monitor for anomalous activity. Vendor tools can assist with the creation and monitoring of baselines
- Establish honey credentials, a large list of fake credentials (that will not work in the organizational environment) that can be 'fed' to phishing campaigns. These honey credentials can be used to profile threat actors and determine their attack source

For more detail about example incident response plays consider reviewing HICP Technical Volume 2, Practice 8: Security Operations and Incident Response.[13]

Enhance Response Capabilities

The incident response team may be formal, or an ad hoc virtual team based on the incident. Regardless of a formal or ad-hoc team, members should be trained on the organization's incident response processes ahead of a crisis. For more information about how to set up an incident response process, review Appendix A: General Incident Response.

Incident response teams need an ability to act so that threats may be prevented and contained. Remediation through eradication and recovery may often involve other groups but containment is often quick and decisive.

The Incident Response team should consider the following actions:

- Remove malicious e-mail messages, files, or attachments from email systems
- Immediately reset user account passwords that have fallen prey to phishing attacks, and reset all active connections associated with stolen credentials
- Feed phishing attacks with honey credentials and track the source IPs that are attempting to access your organization's assets
- Remove endpoints from the network (wired, wireless and remote) that are identified with malware
- Update firewall rules and block known malicious IP addresses detected through your detection mechanisms
- Update signatures to detect and block malicious files or traffic before it can access or execute on a host
- Block malicious domains and IP addresses so that hosts cannot resolve and communicate with those remote endpoints

4. Take Care of the Team

Teamwork effectiveness and efficiency is a priority and might become critical as the situation could be dynamic and evolving during a crisis. Events might last for an indefinite period and impact normal operations for some time. Organizations will need to assess the ever-changing current status of the team. This will ensure that plans can adapt to the remote work environment to continue business operations and that the safety and well-being of the entire team is protected while maintaining privacy among employees.

[13] Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organization
https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol2-508.pdf

During a crisis, health, well-being, job security, and financial stability are top concerns of employees. An organization can address these concerns by communicating such importance directly with employees and sharing what the organization will do to support them during unfolding events.

Communication

Determine how the organization will communicate, leveraging the plans outlined in the first section on Education and Outreach. Crisis Communications or incident notifications are critical to keep staff engaged and productive. Consider the following options:

- Identify primary and backup communication tools and plans with your team. Alternate call tree, texting, or personal e-mail accounts should be considered if the primary accounts fail. Cloud based communication systems can be considered for availability
- Establish a communication platform that can provide informal and on-going collaboration and conversation. Secure instant message, chat and video capabilities can keep employees connected and supplement the social interaction of a team
- Establish a regular meeting cadence for group and individual conversations and tailor information to employee sub-groups as needed

Roles & Responsibilities

Provide clarity for staff on their roles and responsibilities during a crisis or incident to reduce anxiety and frustration. Consider the following options:

- Clearly define staff roles, especially changes which result from the crisis
- Communicate staff responsibilities within and outside of your department to appropriate stakeholders
- If needed, secure temporary staffing to supplement workforce roles

Employee Well-Being

Monitor individuals' condition and their environment; stay in touch with your people and hear their concerns. Consider the following options:

- Ensure communication addresses employee and family needs of those impacted by the event. Employees may need additional time or may not be able to fully engage in their work
- Create a two-way communication channel to solicit feedback from the team on a regular cadence to ensure the needs of employees are met
- Monitor and limit work shifts to less than 12 hours if feasible. Problems associated with long shifts include a disturbed body-clock, shortened and distorted sleep, more errors, reduced productivity and morale, and disturbed family and social life. Ideally, a regular work schedule of 8-10-hour days is preferred
- Communicate the prioritization of employee's well-being to reduce burnout, keep employees engaged to reduce stress

Remote Work

Assess the need for remote work. Consider the following options if events require a remote workforce.

- Share remote work tips and tricks: develop and set activity schedules, suggest creating a designated workspace and setting work/life balance while encouraging exercise and breaks
- Provide meeting and secure communication guidance along with remote data and information security procedures
- Consider referencing existing organizational policies and leverage those for remote work activities
- Acknowledge and recognize that remote work might increase isolation anxiety
- Ensure employees feel appreciated
- Provide employees necessary equipment, resources, tools, connectivity or possibly temporary workspace
- Assign projects and tasks requiring collaboration with other team members to keep employees connected
- Consider offering additional training, townhalls or guest speakers to help employees feel engaged, and support continuous learning

Organizational Self-Assessment

It is important to evaluate the current state of an organization while managing a crisis. At event onset perform an honest and pragmatic assessment of the organization's capabilities to respond by considering the following items:

- The nature of the crisis or threat and the likely key capabilities an organization will need to coordinate.
- The level of maturity / capability of the organization's processes for:
    - Incident Response
    - Emergency Communications (Internal and External)
    - Business Continuity & Disaster Recovery
    - Infrastructure Expansion and Deployment
    - Risk Assessment
    - Change Management
- The resources, internal and external to the organization, that can be made available to work on mitigating issues associated with the crisis while minimizing impact to clinical care.

It is highly likely that cybersecurity teams will be pressed to move quickly into areas not previously considered during a crisis. This will mean expediting activities such as:

- Security Risk Assessments
- Onboarding Resources (internal and external)
- Connectivity to New Partners and Access Control
- Software and Technology Deployments

Coordination with stakeholders within the organization to determine what key activities need expedited paths can reduce the time needed to bring new capabilities online, deploy new processes, and manage the incremental risk associated with rapid large-scale change.

Available Resources

This guide was written by leveraging the vast amount of resources already available through multiple channels. Some of the important resources available are highlighted below:

Health Sector Coordinating Council (HSCC)

The Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG)[14] is a government-recognized critical infrastructure industry council 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.

Health Industry Cybersecurity Practices (HICP)

To strengthen the cybersecurity posture of the HPH Sector, Congress enacted the Cybersecurity Act of 2015 (CSA), Section 405(d), which directed the U.S. Department of Health and Human and Services (HHS) to work with the healthcare sector to "Align Healthcare Security Approaches". In response, HHS convened the 405(d) Task Group, in partnership with the HSCC and the Government Coordinating Council, to develop a set of consensus based and cost effective cybersecurity best practices that can be utilized any size health organization.

The 405(d) program aims to raise awareness, provide vetted cybersecurity practices, and move organizations towards consistency in mitigating the current most pertinent cybersecurity threats to the sector. The 405(d) program developed and published the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) publication.[15] This publication highlights the top 5 cybersecurity threats and the ten best practices organizations of all sizes can implement to mitigate them. In order to continue spreading awareness across the HPH sector the 405(d) Program creates cybersecurity awareness materials including: cybersecurity webinars, awareness posters, in-person town halls, 405(d) Post, and a number of other cybersecurity engagement activities. To receive any of the 405(d) cybersecurity awareness materials for your organization and to engage with the 405(d) Program, contact cisa405d@hhs.gov or check out @ask405d on Facebook, Twitter, or Instagram.

- **Health Industry Cybersecurity Management Checklist for Teleworking Surge During COVID-19 Response**

  An Ad Hoc HSCC Task Group, it establishes a set of working from home considerations in response to the COVID-19 pandemic. This checklist focuses on establishing parameters and considerations for working from home.[16]

- **HIC-MISO / ISBP**

  A HSCC Task Group, it established two documents related to cybersecurity information sharing. The first document is the Health Industry Cybersecurity Information Sharing Best Practices (HIC-ISBP) guide.[17] This guide offers methods of consuming and using threat intelligence information.

---

[14] Healthcare and Public Health Sector Coordinating Council www.healthsectorcouncil.org
[15] Health Industry Cybersecurity Practices (HICP) https://www.phe.gov/405d
[16] Management Checklist for Teleworking Surge During COVID-19 Response https://healthsectorcouncil.org/covid-checklist/
[17] Health Industry Cybersecurity Information Sharing Best Practices https://healthsectorcouncil.org/info-sharing-guide/

The second guide produced was the Health Industry Cybersecurity Matrix of Information Sharing Organizations (HIC-MISO).[18] This guide summarizes many of the Information Sharing organizations that exist, their capabilities and how best to use them.

Health-ISAC

The Health-ISAC is a global, non-profit, member-driven organization offering healthcare stakeholders a trusted community and forum for coordinating, collaborating and sharing vital physical and cyber threat intelligence and best practices with each other. H-ISAC offers a number of resources to the Healthcare community as well as its members. Sector resources include White and Green cyber and physical security alerts, white papers, blogs, newsletters, daily cyber and physical reports and educational webinars, events and videos.

Health-ISAC members receive and share relevant, timely, actionable and reliable information on threats, incidents, and vulnerabilities that can include data such as indicators of compromise, tactics, techniques and procedures (TTPs) of threat actors, advice and best practices, mitigation strategies and other valuable information via machine to machine and human to human sharing. H-ISAC also fosters the community through educational webinars, workshops, exercises and Summits across the globe. Members are offered a variety of tools at little or no cost to help enhance their cyber security and are able to focus on and address topics of importance to the sector through committees and working groups.

HHS Health Sector Cybersecurity Coordination Center (HC3)

The United States Department of Health and Human Services (HHS) formed the Health Sector Cybersecurity Coordination Center (HC3) to harness collaboration among public and private organizations, act as a "central point" for cybersecurity information-sharing, and assist in the identification of threats against the healthcare and public health (HPH) sector. The HC3 publishes threat briefings, sector alerts and whitepapers on cybersecurity issues that directly or indirectly affect the HPH sector. HC3 publications are distributed through its listserv and in coordination with sector partners like the H-ISAC ,HSCC, sector trade associations and consultancies, and with federal partners such as HHS Assistant Secretary for Preparedness and Response (ASPR) through its critical infrastructure protection newsletter. To engage directly with the HC3 or to be placed on a mailing list to receive products or invitations to monthly sector briefings, contact HC3@hhs.gov.

Cybersecurity and Infrastructure Security Agency (CISA)

As the nation's risk advisor, CISA brings our partners in industry and the full power of the federal government together to improve American cyber and infrastructure security. More resources are available below and at cisa.gov.

[18] https://healthsectorcouncil.org/hic-miso/

Resource	Details	Link
Cyber Incident Reporting	Reporting Cyber Attacks to the Federal Government	https://www.dhs.gov/sites/default/files/publications/Cyber%20Incident%20Reporting%20United%20Message.pdf
Report Incidents, Phishing, Malware, or Vulnerabilities	Reports are shared back out to the community	https://www.us-cert.gov/report
Coronavirus		https://www.cisa.gov/coronavirus
Teleworking Guides	DHS/CISA teleworking guides	https://www.cisa.gov/sites/default/files/publications/CISA-TIC-TIC%203.0%20Interim%20Telework%20Guidance-2020.04.08.pdf
Cybersecurity	DHS/CISA's role in cybersecurity	https://www.cisa/gov/cybersecurity
CISA Insights: Risk Management for Novel Coronavirus:		https://www.cisa.gov/sites/default/files/publications/20_0318_cisa_insights_coronavirus.pdf
Cybersecurity Assessments:	DHS/CISA free assessments offered	https://www.cisa.gov/cybersecurity-assessments
Cybersecurity Training and Exercises:	DHS/CISA free training exercises offered	https://www.cisa.gov/cybersecurity-training-exercises

Cyber Insurance	DHS/CISA write-up on cyber insurance	https://www.cisa.gov/cybersecurity-insurance
COVID-19 Exploited by Malicious Cyber Actors	Specific alerts related to COVID-19	https://www.us-cert.gov/ncas/alerts/aa20-099a https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams https://www.cisa.gov/sites/default/files/publications/20_0318_cisa_insights_coronavirus.pdf https://www.us-cert.gov/ncas/alerts/aa20-073a
CISA Alert: Microsoft Office 365 Security Recommendations	Update and reiteration of recommendation related to O365 Security Observations	https://www.us-cert.gov/ncas/alerts/aa20-120a

Appendix A: General Incident Response Process

When presented with an incident, organizations need to ascertain situational "ground truth" to properly assemble appropriate resources. Determination of scope and impact is crucial so that the Incident Command Structure can be activated to mitigate any further damage and to work towards a quicker resolution and restoration of normal business processes. The leader of an incident response team, or the incident commander, along with an identified backup or alternate incident commander, needs to have the authority in advance to make decisions, allocate resources, and take whatever immediate actions necessary. The response leader may be interfacing with a larger organizational incident command team with a broader responsibility, and possibly external response teams in coordination with government agencies such as Federal Emergency Management Agency (FEMA), HHS, and CISA. To be successful the team will need to be able to allocate resources and stakeholders from other functional areas both internal and external to the organization such as:

- Impacted business units
- Communications, Public Relations and Marketing
- Legal Counsel
- Human Resources
- Compliance
- Cyber liability insurance services
- Forensics firm
- Key vendors
- Auxiliary staffing
- Law enforcement

Much has been written around incident response processes and best practices. Those processes typically share components of Preparation, Detection, Analysis, Containment, Eradication, Recovery, and Post Incident Assessment such as is found in NIST 800-61r2. As an organization experiences an incident, it is important to evaluate current status often with accurate notes for possible later use. Timelines; capturing and preserving evidence; possibilities for lessons learned; documentation of time spent; tracking extra unbudgeted monetary expenses and preserving records and observations will be invaluable later when the incident is moving into a post incident analysis phase. Record keeping might also be required for any civil or criminal court actions that may result from the incident.

Visibility into host, network, application, and physical events that occurred as part of an incident is invaluable to incident response teams in the detection and analysis of a potential incident. In order to augment existing visibility, an inventory of available tools and resources should be taken for future process improvement discussions.

Current logging resources should provide an appropriate level of detail for events from hosts, network devices and applications. Make sure the data being collected have identifiers, such as IP address, port numbers, hostname, username, and timestamps at a minimum. Also consider installing centralized log collection with either open source or purchased solutions.

Once centralized logging is operational, consider adding more log sources as they are feasible. Logs from firewalls, active directory, web servers, Citrix servers, PowerShell use on Windows servers, endpoint logging (where feasible), virtual private network (VPN) access, file share access, and any logging available from cloud services your organization uses can all contribute to visibility for incident response activities.

Data loss prevention (DLP) systems also provide pertinent information on possible data exfiltration (intentional or accidental) of sensitive information or an inventory of that information in the network. Although these systems have to be tuned to look for specific data types, they are very effective at locating SEI, PHI, Research, or any type of data you can define. An inventory of where sensitive data are stored provides information security and privacy staff with monitoring targets and alerting that sensitive data have left the network can prove invaluable as well.

Malware detection and prevention are crucial to securing servers and PCs on the network. Many current applications provide visibility into individual host processes and are based on behavior, not just matching signatures of files. These types of newer behavior based anti-malware applications are becoming better at finding those intruders that "live off the land" by using legitimate files and services to infect computers.

Netflow data will show network connections between hosts, the direction of the traffic and the amount of data that was moved. Using NetFlow can be challenging due to the large amount of data generated that has to be stored for analysis. However, if it can be deployed it provides valuable information for incident responders.

Collection and Preservation of Digital Evidence

Following a cyberattack, there is a need for investigating, analyzing and recovering critical forensic digital data from the networks involved in the attack—this could be the Internet and/or a local network -- in order to identify the authors/source of the digital crime and their intentions. Due to legal implications associated with the collection of digital evidence, organizations should have a forensic readiness plan in place which ensures that in the event digital evidence is required, it will be readily available and in an acceptable form. This requires the training of staff and having proper policies in place to ensure compliance. At a high level:

- Organizations should ensure that their policies contain clear statements addressing all major forensic considerations, such as contacting law enforcement, performing monitoring, and conducting regular reviews of forensic policies and procedures
- Organizations should have established relationships and points of contact with entities such as their FBI Cyber Crime Field Office[19] and the National Cyber Forensics & Training Alliance[20] to seek guidance and advise on managing cyber incidents
- Organizations should identify and implement appropriate tools for the secure collection and archiving of appropriate and relevant logs for their information technology environment. (infrastructure, services, applications, user activities and etc.) The tools should ensure the chain of custody requirements required to provide assurance that digital evidence has been gathered, processed, handled and stored with due care such that it is not altered or destroyed. NIST SP 800-92, Guide to Computer Security Log Management,[21] can be used as one of the sources to assist organizations in understanding the need for sound computer security log management.

NIST publication SP 800-86[22] provides practical guidance on performing computer and network forensics. It can be used as a source for organizations in investigating computer security incidents and troubleshooting information technology (IT) operational problems such as the processes for performing effective forensics activities, data sources, including files, operating systems (OS), network traffic, and applications.

The process for performing digital forensics comprises the following basic phases listed below. It is important to ensure the organization's plan for performance of digital forensics is in concert with law enforcement support teams such the organization's local FBI Cyber Crime Field Office:

COLLECTION: Identifying, labeling, recording, and acquiring data from the possible sources of relevant data, while following procedures that preserve the integrity of the data.

EXAMINATION: Forensically processing collected data using a combination of automated and manual methods, and assessing and extracting data of particular interest, while preserving the integrity of the data.

ANALYSIS: Analyzing the results of the examination, using legally justifiable methods and techniques, to derive useful information that addresses the questions that were the impetus for performing the collection and examination.

REPORTING: Reporting the results of the analysis, which may include describing the actions used, explaining how tools and procedures were selected, determining what other actions need to be performed (e.g., forensic examination of additional data sources, securing identified vulnerabilities, improving existing security controls), and providing recommendations for improvement to policies, procedures, tools, and other aspects of the forensic process.

NOTIFICATION: Notifying Federal agencies and law enforcement entities of the incident and requesting assistance to investigate the incident. The "Cyber Incident Reporting, A Unified Message for Reporting to the Federal

---

[19] FBI Cyber Crime https://www.fbi.gov/investigate/cyber
[20] National Cyber Forensics & Training Alliance https://www.ncfta.net/
[21] NIST SP 800-92, Guide to Computer Security Log Management https://csrc.nist.gov/publications/detail/sp/800-92/final
[22] NIST: Guide to Integrating Forensic Techniques into Incident Response https://csrc.nist.gov/publications/detail/sp/800-86/final

Government"[23] provides information about when, what, and how to report to the Federal Government in the event of a cyber-incident, mitigate its consequences, and seek help to prevent future incidents. Federal law enforcement agencies have highly trained investigators who specialize in responding to cyber incidents for the express purpose of disrupting threat actors who caused the incident and preventing harm to other potential victims. In addition to law enforcement, other federal responders provide technical assistance to protect assets, mitigate vulnerabilities, and offer on-scene response personnel to aid in incident recovery.

Citations

COVID-19 Exploited by Malicious Cyber Actors

- https://www.us-cert.gov/ncas/alerts/aa20-099a

CISA: Cybersecurity

- https://www.cisa.gov/cybersecurity

How to: Block legacy authentication to Azure AD with Conditional Access

- https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication

Health Industry Cybersecurity Information Sharing Best Practices

- https://healthsectorcouncil.org/info-sharing-guide/

Cabby

- https://www.eclecticiq.com/open-source/cabby

Minemeld

- https://github.com/PaloAltoNetworks/minemeld/wiki

H-ISAC

- https://h-isac.org/

Automated Indicator Sharing (AIS)

- https://www.us-cert.gov/ais

InfraGard

- https://www.infragard.org/Application/Account/Login

Internet Storm Center: Threat Feeds

- https://isc.sans.edu/threatfeed.html

Health Industry Cybersecurity – Matrix of Information Sharing Organizations (HIC-MISO)

- https://healthsectorcouncil.org/hic-miso/

Spamhaus

- https://www.spamhaus.org/

Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations

- https://www.phe.gov/Preparedness/planning/405d/Documents/tech-vol2-508.pdf

Healthcare and Public Health Sector Coordinating Council

- www.healthsectorcouncil.org

Health Industry Cybersecurity Practices (HICP)

- https://www.phe.gov/405d

[23] Cyber Incident Reporting, A Unified Message for Reporting to the Federal Government https://www.dhs.gov/sites/default/files/

Management Checklist for Teleworking Surge During COVID-19 Response

- https://healthsectorcouncil.org/covid-checklist/

Health Industry Cybersecurity Information Sharing Best Practices

- https://healthsectorcouncil.org/info-sharing-guide/

Traffic Light Protocol (TLP) Definitions and Usage

- https://www.us-cert.gov/tlp

FBI Cyber Crime

- https://www.fbi.gov/investigate/cyber

National Cyber Forensics & Training Alliance

- https://www.ncfta.net/

NIST SP 800-92 Guide to Computer Security Log Management

- https://csrc.nist.gov/publications/detail/sp/800-92/final

NIST: Guide to Integrating Forensic Techniques into Incident Response

- https://csrc.nist.gov/publications/detail/sp/800-86/final

Cyber Incident Reporting, A Unified Message for Reporting to the Federal Government

- https://www.dhs.gov/sites/default/files/publications/Cyber Incident Reporting United Message.pdf