



Health Sector Coordinating Council
Cybersecurity Working Group



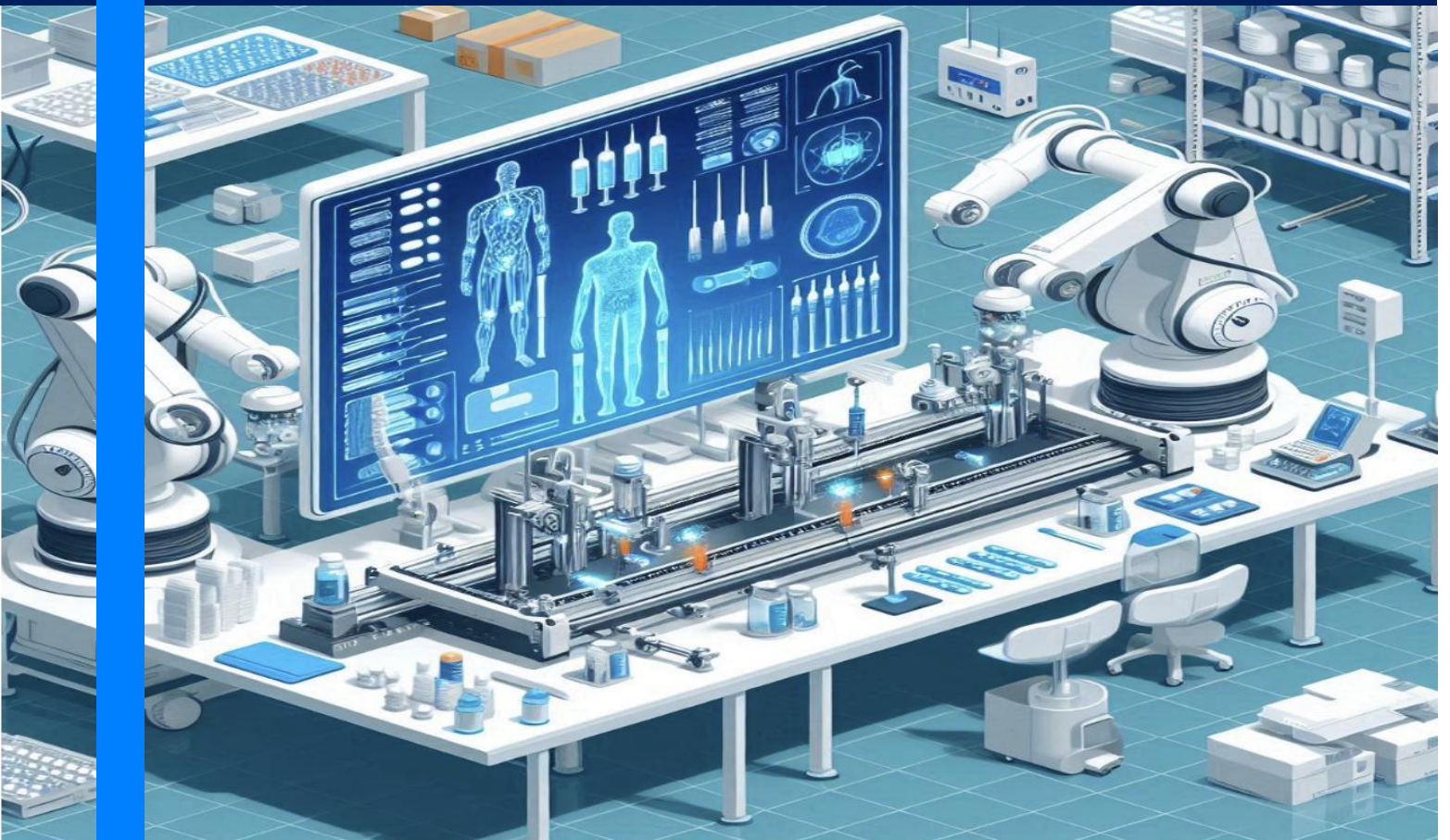
Respond &
Recover



Secure
Medtech

HEALTH INDUSTRY CYBERSECURITY

Medical Product Manufacturer Cyber Incident Response Playbook (MPM CIRP)



NOVEMBER 2024

Table of Contents

Executive Summary	4
About the Health Sector Coordinating Council Joint Cybersecurity Working Group	5
Introduction	5
How to Use the Playbook	6
Summary of Cyber Incident Response Phases	6
Preparation: Building a Cyber Incident Response Plan and Procedures	6
Establish a Cyber Incident Response Team (CIRT)	7
Identify, Develop, and Document Response Personnel and Partners	11
Compile Key Documentation of Business-Critical Networks and Systems	12
Develop Technical Response Procedures for Incident Handling	13
Maintain Procedures to Classify the Severity of Cyber Incidents	13
Develop Strategic Communication Procedures	14
Develop Legal Response Procedures	15
Obtain Buy-In and Sign-Off from Senior Leadership	15
Exercise the Plan, Train Staff, and Update the Plan Regularly	15
Identifying and Digging Deeper: Detecting, Investigating, and Analyzing Incidents	15
Establish a Clear Process for Identifying and Reporting Cyber Alerts	17
Investigate and Declare a Cyber Incident	19
Engaging Help: Activating the Response Team and Engaging Resources	20
Activate the Cyber Incident Response Team	20
Engage Expert Response Resources	21
Take Action: Containment and Eradication	21
Conduct Initial Containment Actions	21
Carefully Capture and Document Incident Information	22

Execute Evidence Gathering, Handling, and Preservation Procedures	23
Report the Incident as Required by Laws, Regulations, and Contracts	24
1. Federal Cyber Incident Reporting Obligations	25
2. Cyber Insurance Contract Requirements (if applicable)	27
Develop Response Solutions and Assess Resource Needs	28
Enact the Response Plan and Eradicate the Threat	28
<hr/>	
Incident Recovery and Post Incident Activity	28
Recover from an Incident	28
Conduct After-Action Review	29
1. Internal Considerations and Actions	29
2. External Considerations and Actions	30
<hr/>	
Appendix A: Resource Matrix and Additional Resources	30
Matrix of Example Sector Resources	30
Additional Cyber Incident Response Related Readings and Resources	33
<hr/>	
Acknowledgements	33

Executive Summary

Medical products—from medical devices, drugs, and biologics to durable equipment and other products—are critical to the delivery of healthcare and public health services. In the increasingly digital world, the manufacturers of these essential products have embraced digital technologies and systems to improve efficiency, reliability, productivity, and other aspects of the medical product processes. However, this increased connectivity and integration comes with cyber risks that may disrupt the manufacturing and operations for these products—cyber risks and associated impacts manufacturers should be prepared to respond.

Consequently, the Healthcare Sector Coordinating Council’s Manufacturing Operational Technology Cybersecurity Task Group—a joint collaborative between government, medical product manufacturers, and other stakeholders to advance manufacturing cybersecurity best practices and resources—sought to develop a resource to address this need and evolving landscape.

The Medical Product Manufacturer Cyber Incident Response Playbook (MPM CIRP) is a comprehensive guide that provides information, step-by-step recommendations, and processes for medical product manufacturers to use in responding to manufacturing cyber incidents.

The MPM CIRP details information and recommendations for stakeholders involved in the production of medical products (e.g., medical devices, pharmaceuticals, biologics)—known as medical product manufacturers. MPM CIRP covers, among other things:

- Detailed recommendations for medical product manufacturers across the following phases of cyber incident response:
 - Preparedness
 - Detection, Investigation, and Analysis,
 - Containment,
 - Eradication, and
 - Recovery and Post-Incident Activity
- Information on relevant stakeholders (e.g., federal, state/local, industry) and other cyber incident response resources relevant to medical product manufacturers.

This Playbook is meant to serve as a starting point for some medical product manufacturers, or an accelerator for others, to create and tailor their own internal playbooks for their specific circumstances—all towards advancing the response and resiliency of medical product manufacturers to cyber incidents.

Scope Statement

The scope of this publication includes various policy, process, and technical best-practice recommendations that are tailored specifically to medical product manufacturing across the cyber incident response phases—from preparation to recovery and post-incident activities. This publication provides information and recommendations within the context of the broader medical product manufacturer enterprise and is not limited to only singular manufacturing facilities. Privacy considerations/requirements and legal guidance are outside the scope of this document.

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 470 healthcare providers, pharmaceutical and medical technology companies, payers, health IT entities and government agencies partnering to identify and mitigate cyber threats to health data and research, systems, manufacturing and patient care. The JCWG membership collaboratively develops and publishes free healthcare [cybersecurity leading practices](#) and policy recommendations, and produces outreach and communications programs emphasizing the imperative that cyber safety is patient safety.

Introduction

Like most modern industries, medical product manufacturing has embraced the use of advanced digital technologies to improve efficiencies, increase reliability, and maximize productivity, including the output of products.

Manufacturing facilities are now highly connected, leveraging complex infrastructure—hardware, software, and machinery—to produce the medical products on which the healthcare sector has come to rely. These manufactured products include medical devices, pharmaceuticals, biologics, biotechnology, durable medical equipment, consumables and single-use items, and other medical products.

The increased integration and connectivity come with many benefits but do not come without risks. As systems are integrated, they raise the exposure to cyber threats that can lead to cyber incidents that have the potential to disrupt critical manufacturing services and operations. Manufacturers must address these risks to build a foundation of resilience.

To ensure a resilient, reliable, and safe flow of medical products, medical product manufacturers must be prepared to proactively identify and manage cyber risk, and—when they occur—effectively and timely address any potential disruption and maintain a resilient supply chain. The Health Sector Coordinating Council (HSCC) Joint Cybersecurity Working Group stood up the Operational Technology Manufacturing Cybersecurity Task Group (OT Manufacturing Cyber TG) to develop resources to help medical product manufacturers manage cyber risk, including the identification of manufacturing cybersecurity best practices and incident response procedures.

This Medical Product Manufacturer Cyber Incident Response Playbook (“Playbook”) provides step-by-step recommendations and processes for medical product manufacturers to use in identifying and responding to manufacturing cyber incidents, from preparation through remediation. The recommendations and procedures are tailored to be applicable across organizations of various sizes and types and provide a basic platform that organizations may use or adapt according to their own needs. This Playbook is meant to serve as a starting point—or accelerator—for companies to create and tailor their own internal playbooks for their specific circumstances.

How to Use the Playbook

The Playbook provides introductory guidance, especially for small to mid-sized, medical product manufacturers to help them prepare for, respond to, recover from, and learn from cyber incidents.

Particularly, the playbook serves several key purposes:

- Provides guidance to help a medical product manufacturer develop its cyber incident response plan as part of preparedness for incidents and related disruptions.
- Provides an outline for responding to cyber incidents by describing the processes and procedures for detecting, investigating, eradicating, and recovering from a cyber incident.
- Maps out the industry and government partners that medical product manufacturers can engage during a cyber incident to share information, get support for incident analysis and mitigation, and coordinate messaging for incidents that require communication with customers and the public.

Summary of Cyber Incident Response Phases

Cyber incident response is not limited to only the reactive activities during an incident but constitutes a greater cycle and feedback loop of activities encapsulating preparedness, response, recovery, and post-incident analysis and improvements. The following points provide a brief description of the main phases of cyber incident response that the playbook follows for later sections:

- **Preparation:** Development of the cyber incident response plan and procedures utilized for the subsequent cyber incident response phases, in addition to training on and practice of those plans/procedures.
- **Detection, Investigation, and Analysis:** Procedures for alerting, detection, escalation, and declaration of a cyber incident. Additionally, procedures for the classification, prioritization, and investigation of a cyber incident.
- **Containment:** Activating the Cyber Incident Response Team, conducting initial containment actions, documenting the incident, establishing procedures for evidence gathering and handling, and conducting required cyber incident reporting.
- **Eradication:** Developing response solutions, assessing resource needs, engaging external resources and response organizations, and following a response plan to eradicate the threat.
- **Recovery and Post-Incident Activity:** Restoring the system to full operation and verifying that mitigation actions were effective. In terms of post-incident activity, lessons learned from the cyber incident are documented and integrated back into the preparation stage of the cyber incident response phase cycle including in medical product manufacturer's cyber and enterprise risk management processes.

Preparation: Building a Cyber Incident Response Plan and Procedures

This section of the playbook identifies key elements that medical product manufacturers should consider when preparing for cyber incidents, including considerations for developing, maintaining, and training in a cyber incident response plan.

While each manufacturer's response capabilities differ, all manufacturers can use the guidance in this playbook section to document a cyber incident response process that can be scaled as appropriate for their organization and ecosystem.

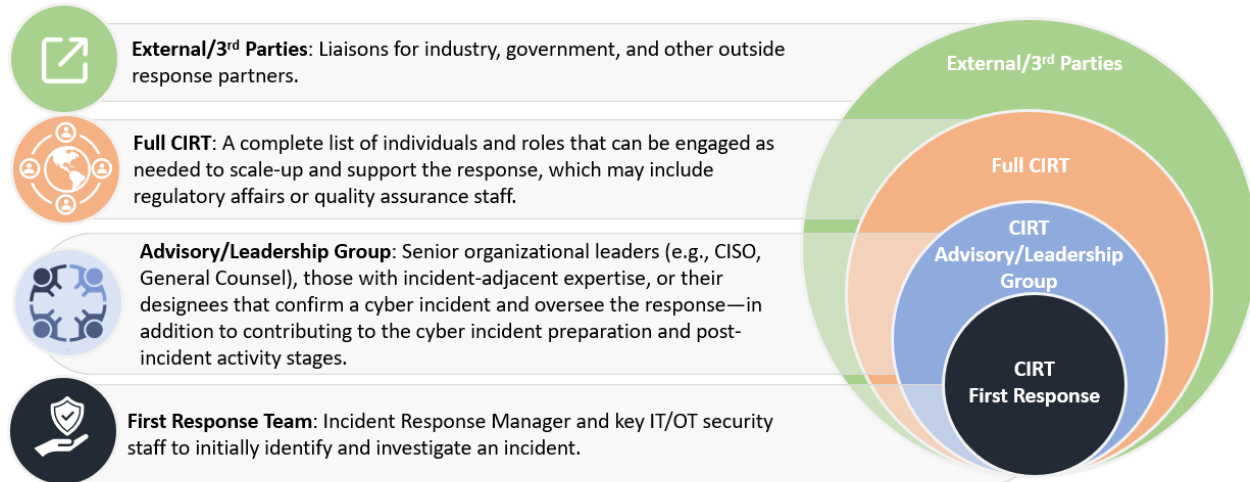
Establish a Cyber Incident Response Team (CIRT)

The most vital component of incident preparation is establishing a team of personnel who have the responsibility and the authority to take action during a cyber incident without delay. The Cyber Incident Response Team (CIRT) includes the individuals responsible for assessing, containing, and responding to incidents, as well as those responsible for product safety or availability, sector resiliency impacts, and physical safety of facilities and personnel; the business and legal impacts; reporting as appropriate; communicating to internal and external stakeholders; and engaging with industry and government response partners to coordinate information and resource sharing when needed.

Larger medical product manufacturers may have dozens of staff assigned to formal technical response and crisis management roles. In contrast, incident response at smaller manufacturers may be led by a few individual information technology/operational technology (IT/OT) and management staff who are familiar with the IT/OT and cybersecurity infrastructure, and who can pull in additional representatives ad hoc from other departments and outside entities as required. Manufacturers may rely on contract manufacturers and other external stakeholders which require additional contractual and practical cooperation considerations to address incident response management.

The specific nature of an incident dictates the size of the incident response team and which capabilities are activated. A tiered structure for the CIRT offers a flexible approach for engaging the right personnel quickly and convening a broader CIRT that fits each incident's response needs. This cascade of structure and individuals is described in the following figure:

Figure 1. Example Cyber Incident Response Team Structure Cascade



Roles and Responsibilities

For many manufacturers, the response effort involves not only the staff of the medical product manufacturer, but also regional or other government, regulatory and third-party resources.

Key team roles may be filled by IT/OT/cybersecurity staff or teams, legal teams, compliance officers, human resources staff, and public affairs or media relations staff. Many manufacturers also contract out cybersecurity services involved in detection and response (such as system monitoring and intrusion detection) and hire third-party, on-call crisis service providers to assist in key areas of incident response, such as forensic analysis and incident mitigation.

These third parties are members of the CIRT and should be included in the cyber response planning. External federal, state, and other agencies may also be involved in the response but are not members of the CIRT.

Particularly at smaller manufacturers, one person may serve in multiple roles on the CIRT. For example, the Cyber Incident Response Manager and IT technical response leads are often the same person. Additionally, the liaison roles may be collapsed, or several liaison roles may be filled by one person.

Small cybersecurity teams can deliver a flexible, agile response—provided roles, responsibilities, and contacts are identified ahead of time. The following table identifies the roles, diverse skill sets, and responsibilities that may be required in a cyber incident and be constituent parts of the Full Cyber Incident Team and subsequent incident response structures. Consider which staff or resources may be required to fulfill these roles, recognizing that an individual may serve multiple roles within the team.

Table 1. Examples of Incident Response Roles and Responsibilities

Cyber Incident First Response Team Roles and Responsibilities

Cyber Incident Response Manager	Manage cyber incidents from detection to recovery and direct response procedures. Declare and categorize cyber incidents. Notify and liaise with senior management. Work with the CIRT Advisory/Leadership Group members to ensure senior management awareness and engagement, in addition to ensuring that the response has the necessary personnel, resources, and skills. Requires a working knowledge of the medical product manufacturer's IT/OT systems, cybersecurity capabilities, and business operations.
IT/OT Technical Responders	Investigate and analyze cyber incidents; and identify and conduct actions necessary to contain, eradicate, and recover from an incident under direction of the Cyber Incident Response Manager. Complete the initial collection and preservation of forensic evidence.
Subject Matter Experts (e.g., medical product, asset owner)	Provide expert advice and guidance regarding cyber incident response activities in terms of specific medical products, manufacturing facilities, manufacturing process, physical safety, impact on patients and customers, and other associated topics/processes that are outside of IT/OT technical security roles.
Senior Manager/ Executive	Assess the business impact of a cyber incident with SME input. Allocate resources or authorize contracted cyber incident services. Communicate with city/state/federal officials in consultation with legal counsel. Determine when to voluntarily engage outside support. A Senior Manager/Executive may include the Chief Information Officer, Chief Information Security Officer (CISO), and/or business line owner.

Other CIRT Roles and Responsibilities

Communications/ Public Affairs Personnel	Support the technical response team in devising messages to appropriately communicate to all relevant stakeholder groups. Proactively communicate and quickly respond to all employee, media, and customer inquiries, in addition to supporting engagements with regulatory authorities and other stakeholders.
Legal Counsel	Assess, advise, and engage on the legal ramifications of a cyber incident and cyber incident response activities including communications and addressing statutory, regulatory, and contractual requirements.
Regulatory Affairs Personnel	Support the assessment of impacts to regulated medical products and necessary compliance activities during a cyber incident response. Communicate with

	regulatory authorities as necessary, in addition to senior management, legal counsel, and communications personnel.
Human Resources Representative	Ensure staff resources to enable 24/7 response operations as directed by the Cyber Incident Response Manager. Assist with managing any communications with employees relating to the cyber incident.
Finance Representative	Appropriately management and allocate funds to CIRT. Assess the cost and business impact of a cyber incident.
Liaison to Senior Executives/Board of Directors	Keep senior leadership and the Board of Directors apprised of the response to the incident, any operational or business impacts, and any internal or external communications. Share the input of the senior leadership and board with the full CIRT.
Cyber Insurance Liaison	Communicate with the insurance company and ensure compliance with policy requirements.
Reporter	Supports the capturing and documentation of cyber incident response activities/actions that occur in order to inform future after-action reviews and development of lessons-learned.

Staffing the Cyber Incident Response Team

Consider the following factors when assessing CIRT staffing needs:

- **24/7 Availability:** Designate and train backup roles for critical staff, as incidents may occur during off-hours or vacations for lead staff. Some cyber incidents may require around-the-clock response, which can quickly tax incident response employees. Lead and backup roles may need to work in shifts or require contract resources or service providers to supplement staff roles.
- **Cost and Training:** Manufacturers should account for not only compensation but also the cost of training and maintaining cyber incident response skills when assessing incident response planning budgets.
- **Staff Expertise:** Incident handling and mitigation often require specialized knowledge and experience. Third-party experts can provide on-call intrusion detection, investigation, forensics, and recovery services to supplement in-house skill sets.

Build from the manufacturer's all-hazards incident response plan or other emergency risk management/response plans when identifying the cyber incident response team. First, several response roles that are required in any type of incident (e.g., human resources, logistics, and many liaison roles) may already have clearly defined responsibilities, authorities, and personnel. Second, these plans may have accounted for staffing considerations of large events, including staffing a 24/7 response operation, compartmentalizing roles to minimize oversight from key staff, assessing response cost, and maintaining employee morale during taxing multi-day incidents.

Ensure CIRT members have the necessary authority to act. Cyber incidents can be fast-moving, requiring rapid decision-making by a small team of people with little time to seek authorization for important response activities. Consider in advance what authorities CIRT team members will need:

- Who on the CIRT has the authority to make critical decisions to contain a cyber incident, such as to isolating/disconnecting key business and operational networks or shutting down manufacturing lines?
- Who is authorized to request additional support from service providers? What resource procurement processes must be followed?
- Who has the authority to report a cyber incident? Who will interface with external incident response partners (e.g., suppliers, customers, ISACs, regulators, public health, etc.)?
- Who will ensure compliance with mandatory reporting requirements and notify government officials and regulatory bodies?
- Who will report a suspected criminal attack to law enforcement and submit mandatory paperwork to regulatory bodies?
- Who will be the public face for this incident, and who has the authority to communicate with the press and the general public?

In total, it is critical for medical product manufacturers to establish a clear group of personnel responsible for responding to cyber incidents, ensure that staff understand their roles in a response team, and plan for the resources and authority necessary to empower those individuals in an incident response.

Identify, Develop, and Document Response Personnel and Partners

Identify Response Partners and Resources

Many medical product manufacturers lack a clear strategy to engage outside resources if an incident overwhelms the cyber response resources and expertise of their cybersecurity staff/contracted cybersecurity service providers. Identifying how to engage external response organizations, signing non-disclosure agreements, retaining necessary cybersecurity response organizations and experts, and reviewing legal agreements in advance of an incident can save precious time in a future incident.

See Section IV. Engaging Help: Activating the Response Team and Engaging Resources outlines considerations for engaging industry and government partners that medical product manufacturers can integrate into their incident response plans.

Develop and Maintain a 24/7 Contact List for Response Personnel and Partners

Medical product manufacturers should develop and regularly update contact lists for incident response team personnel, vendors, and security service providers that may be on call during an incident. Additionally, up-to-date contacts should be maintained for external partners that can provide aid or information at crucial junctions during response as well as external entities that may require notification to meet regulatory reporting requirements.

Establishing this contact in advance can help incident managers, IT personnel, and management alert and engage resources early, even without a formal incident response plan in place. This list should contain the names, roles,

primary contact information, backup contact information, and potential alternates for each role. It should be maintained online and in a central, offline location (e.g., physical binder, offline computer) circulated widely among the incident response parties.

Contact lists can include:

- Internal stakeholders such as:
 - Departmental leads on the incident response team (senior management, IT/OT security, operations personnel, communications/public affairs, legal representatives, etc.).
 - CISO and IT security department for state/local jurisdictions.
- Support contacts for all software and equipment suppliers and contracted service providers. Identify the authorized support contact personnel, the type of support expected and contractual requirements for:
 - Critical system vendors, who can provide information on the significance of log entries or help identify false positives for certain intrusion detection signatures.
 - Internet service provider (ISP), who can provide requested information about major network-based incident information, identify potential origins, or potentially block communication pathways as requested.
 - Contracted security service providers for monitoring, investigation, forensics, and response, as applicable.
 - Insurance brokers and other legal or business resources to support business continuity.
 - Utility companies (i.e., communication, power, water) that may provide services to the manufacturer and its local facilities.
- Key contact or liaisons for industry and government response partners:
 - Cybersecurity liaisons at law enforcement agencies (e.g., Federal Bureau of Investigation [FBI], state/local agencies as appropriate)
 - Incident reporting and information-sharing organizations (e.g., ISAC/ISAO, DHS)
 - Federal response agencies (e.g., U.S. Department of Health and Human Services [HHS] including the U.S. Food and Drug Administration [FDA] and U.S. Department of Homeland Security [DHS] Cybersecurity and Infrastructure Security Agency [CISA]).
 - State, local, tribal, and territorial government fusion centers
 - Cyber insurance providers
 - External cyber incident response teams (including those that a manufacturer may have contractually retained)
- Key contacts for outside legal counsel.

Compile Key Documentation of Business-Critical Networks and Systems

Documenting the following information prior to an incident is especially helpful if an incident occurs when the primary management team is unavailable, or if additional vendor support or expertise must be pulled in to manage a significant or fast-moving cyber event:

- An inventory of the IT/OT systems and networks that support core business and operational processes can help to quickly investigate the extent of an incident and assess potential impacts. For each application or process, identify the owner and which IT/OT assets, systems, and network connections support it.

Assigning a business priority for recovery can establish the order in which systems should be restored. This inventory and business impact analysis to inform system criticality/recovery priority may be completed by a third party.

- Network scheme displaying the network architecture with internal network segmentation and the various gateway networks, as well as the range of network perimeters (i.e., demilitarized zone [DMZ]), virtual paths (VP), and internet protocol (IP) addresses used. Network maps can help quickly orient cyber management teams.
- Equipment and configuration inventory of core assets in medical product manufacturing environment as well as server and network components used to deliver corporate and operational services. This inventory not only supports risk management but it also enables IT personnel to quickly determine whether a newly discovered vulnerability or incident could affect the manufacturer's equipment, the potential extent of compromise, and the processes or functions that could be affected.
- Location of and access to critical backup data as well as instructions for restoration.
- Documentation of baseline traffic patterns so that anomalies are easily identified.
- Account permission list to discern who has the authorization to access, use, and manage the manufacturer network and the various systems within it. This will help IT and OT personnel investigate and confirm unauthorized access and remove access to isolate an incident.
- Documentation of prior penetration testing results, if available.

Develop Technical Response Procedures for Incident Handling

The medical product manufacturer should develop a detailed list of response processes—designating which CIRT members act and when—for all phases of a cyber incident (i.e., preparation; detection, investigation, and analysis; containment; eradication; and recovery and post-incident activity). This should include activities such as restoration from backup data as well as capturing and preservation of forensic evidence.

For more details, see Section III. Identifying and Digging Deeper: Detecting, Investigating, and Analyzing Incidents for guidance on response steps and considerations for technical elements of cyber incident responses.

Maintain Procedures to Classify the Severity of Cyber Incidents

It is helpful for medical product manufacturers to have a framework to categorize the severity of a cyber incident. Using common severity levels can help the CIRT quickly mobilize the right resources based on the type of incident and convey the potential impacts when notifying internal and external stakeholders. “Sample Cyber Incident Severity Levels” provides a sample schema from the 2016 National Cyber Incident Response Plan to categorize cyber incidents, considering the functional impact, information impact, and recoverability effort that typically characterize these incidents. The table shows an example incident severity schema for national cyber incidents commonly used among federal cyber response organizations.

Figure 2. Example Cyber Incident Severity Schema from National Cyber Incident Response Plan (2016).

General Definition		Observed Actions	Intended Consequence ¹
Level 5 <i>Emergency</i> (Black)	<i>Poses an imminent threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.</i>	Effect	Cause physical consequence
Level 4 <i>Severe</i> (Red)	<i>Likely to result in a significant impact to public health or safety, national security, economic security, foreign relations, or civil liberties.</i>		Damage computer and networking hardware
Level 3 <i>High</i> (Orange)	<i>Likely to result in a demonstrable impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.</i>	Presence	Corrupt or destroy data
Level 2 <i>Medium</i> (Yellow)	<i>May impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.</i>		Deny availability to a key system or service
Level 1 <i>Low</i> (Green)	<i>Unlikely to impact public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.</i>	Engagement	Steal sensitive information
Level 0 <i>Baseline</i> (White)	Unsubstantiated or inconsequential event.	Preparation	Commit a financial crime Nuisance DoS or defacement

Each manufacturer may define severity levels that best reflect their design, operations, and potential impacts (e.g., IT, OT, business impacts); however, utilization of existing severity schema can assist in harmonizing communication with external response stakeholders. Overall, procedures should be developed to classify the severity of an incident to ensure appropriate communication, mobilization of resources, and timeliness of response activities.

See Section III. Identifying and Digging Deeper: Detecting, Investigating, and Analyzing Incidents for further discussion of cyber incident impacts that will contribute to the severity classification of an incident.

Develop Strategic Communication Procedures

Information sharing policies and procedures should be developed with input from the manufacturer’s public affairs/communications department, legal department, and senior management. The aim is to control communication flow to ensure the right information is communicated at the right time by the right personnel, through approved channels, to the right stakeholders. The nature of the incident will determine the type of communication required, however, the principle of “need to know” should be respected internally.

Develop Legal Response Procedures

A medical product manufacturer's legal team must be central to its cyber incident response plan. Manufacturers should develop Cyber Incident Legal Response Procedures, and promptly alert the legal team of a cyber incident. To ensure compliance and preserve the manufacturers' legal posture, legal counsel should be closely involved in incident investigation, documentation, and reporting processes.

Obtain Buy-In and Sign-Off from Senior Leadership

Review the contents of the incident response plan with senior management and obtain their buy-in with signature forms. Senior management should review the roles and responsibilities of the cyber incident response team and approve the authorities of key team members during incident response.

Exercise the Plan, Train Staff, and Update the Plan Regularly

A cyber incident response plan on paper has little value if cyber incident responders do not understand their roles and exercise response steps regularly—ideally at least once per year. The medical product manufacturer should convene key members of the organization's CIRT, train them on processes and procedures, and conduct exercises or participate in industry exercises to test the plan.

Activities to exercise the plan, train staff, and maintain the plan can include:

- Test a variety of different scenarios and impacts to identify gaps in procedures or staff capabilities.
- Conduct abbreviated exercises during plan development to help generate discussions on roles, authorities, and response procedures. In between exercises, conduct drills with small teams of employees to reinforce their roles and identify training needs.
- Practice incident documentation during exercises, including using incident handling forms, preserving forensic images, and accessing and investigating logs.
- Review and update the incident response plan annually (especially contact sheets and other variable information) and as part of any post-incident review (as described in Section VI.B).
- Ensure that gaps in response roles due to staff turnover are filled by trained new or existing staff, in addition to ensuring that new staff are appropriately trained and included in response exercises/preparations.

Identifying and Digging Deeper: Detecting, Investigating, and Analyzing Incidents

This section contains guidelines and considerations for medical product manufacturers as they develop detailed technical response procedures for the key phases of incident response.

One of the most challenging aspects of the cyber incident response process is determining whether an incident has occurred, and if so, the type and magnitude of the incident. Cyber incident alerts typically come in the form of indicators of compromise (IOC)—as a sign that a cyber incident may occur, has occurred, or is currently occurring. These IOCs can be of two types: internal IOCs and external IOCs. Additionally, the IOCs can be specific to the types of technologies in manufacturing environment—for example, they can be different in the context of IT versus OT.

Internal IOCs are alerts of cyber incidents that are identified by internal monitoring systems, personnel within a manufacturer, or other internal sources. For example:

- IT-Related Internal IOCs
 - A network administrator notices uncommon fluctuations in network traffic flows.
 - Firewall or antivirus software alerts.
 - An application records multiple failed login attempts from an unfamiliar remote system.
- OT-Related Internal IOCs
 - Manufacturing floor equipment ceases to operate as intended or maintain the expected operational level.
 - The quality and/or quantity of the manufacturing output is unexpectedly reduced.
 - Unexpected variability in industrial control systems or processes is observed including unusual network traffic in the industrial control system network.
 - Latency in operational systems is observed.

External IOCs are alerts of cyber incidents from external sources such as federal agencies, private cyber threat intelligence organizations, peers in the sector, or other stakeholders. For example:

- IT-Related External IOCs
 - A medical product manufacturer receives a ransomware prenotification from a federal agency.
 - An information sharing and analysis center (ISAC) releases an alert on threats to a specific group of member manufacturers.
 - A manufacturer or external partner notifies a peer medical product manufacturer of suspicious activities regarding the peer's systems.
 - External party connected to a manufacturer via Virtual Private Network (VPN) reports a compromise of the VPN by a threat actor.
- OT-Related External IOCs
 - Customer reports unexpected quality issues with the product.
 - Notification from an operational technology provider that it is aware of cyber incidents impacting other customers or another infrastructure sector utilizing that equipment.

It is important to understand common threat vectors and develop a clear process for identifying and reporting cyber alerts to the information/operations security team or other appropriate party. Those reports can allow responsible teams to analyze cyber alerts and notify the Cyber Incident Manager or other responsible individuals of potential incidents.

Table 2. Examples of Cyber Threats

Source or Vector	General Description	Example
Compromised Remote Access	A threat stemming from compromised remote access software that allows connection to or access to a computer, network, or other system remotely.	Stolen credentials are utilized to access a Virtual Private Network (VPN) that connects to a firm's networks.
External or Removable Media	A threat introduced via a removable or external device.	An infected USB drive introduces malware.
Attrition	A threat that uses brute force techniques to compromise systems, credentials, networks, or applications.	Continuous attack (e.g., Denial of Service).
Web	A threat carried out from a website or web-based application.	Website installs malware on workstation.
Email	A threat carried out through a phishing email with a malicious link or attachment.	The body of an email message from a known address contains a link to a malicious website.
Impersonation	A threat that inserts malicious processes into something benign.	Rogue wireless access points.
Improper Usage	A threat stemming from user violation of manufacturer's usage policies.	An employee installs file-sharing software.
Loss or Theft of Equipment	Loss or theft of proprietary device used by an organization.	A stolen workstation provides unauthorized actors access to sensitive customer data.

**Note: MITRE ATT&CK provides a globally accessible, common means of categorizing/describing cyber threat tactics and techniques through its various matrices and resources, including those for enterprise and industrial control system contexts. Visit attack.mitre.org for more information.*

Establish a Clear Process for Identifying and Reporting Cyber Alerts

Threat precursors and indicators can be identified through several channels, including suspicious activity reported by a medical product manufacturer's employees, alerts from intrusion detection systems and other monitoring systems, review of system logs, and Indicators of Compromise (IOCs) or other indicators from threat/vulnerability databases. The team should have a process for reviewing and escalating alerts for further investigation.

Personnel Detection

Identify and train all staff on reporting mechanisms for suspicious activity or other indicators, such as a help desk phone number, email address, secure web form, or instant messaging system to report observations to the information security team. Members of a medical product manufacturing organization should be aware of reporting procedures if they observe something abnormal in their systems or devices.

Detection Software and Monitoring Systems

Develop a system for processing and analyzing alerts from monitoring software or systems, including, but not limited to:

- Intrusion detection and prevention systems, which can identify and record suspicious events, and log critical data to investigate an incident (e.g., date and time of suspected intrusions, source and destination IP addresses).
- Antivirus software monitors networks and scans files for various forms of known malware.
- Third-party security services that monitor real-time system traffic to detect potential events or investigate alerts.
- Firewalls, network monitoring tools, and security gateways.

If a medical product manufacturer does not already deploy detection and monitoring software in which some of these alerts may be generated, acquisition of such systems should be considered.

System Logs

Reviewing logs—including operating system, service, and application logs; network device (e.g., firewall) logs; and logs of network flows—can identify network trends and alert employees to suspicious behavior or help the response team correlate events to verify an incident. Logs provide great value during incident response, as they can provide a record of attacker activity, such as connection attempts, accounts accessed, and what actions took place on critical systems. A security information and event management (SIEM) system/solution may help to support centralized management of system logs for review.

Cybersecurity Alerts

Monitoring alert databases for new threats, vulnerabilities, and exploits can alert the team to potential threat vectors (like newly discovered vulnerabilities) and help identify threat indicators to monitor for (such as IP addresses and behaviors). External entities such as ISACs/ISAOs and CISA provide threat alerts on newly discovered vulnerabilities, threat methods, or threat indicators (see the following table).

Sources of Cyber Threat and Vulnerability Alerts

The U.S. Department of Homeland Security (DHS)'s Cybersecurity and Infrastructure Security Agency (CISA) analyzes cyber threats, vulnerabilities, and exploits and disseminates cyber threat alerts through several channels:

- Cybersecurity Alerts that focus on concise cybersecurity topics for common computing systems and devices.
- ICS Advisories that focus on industrial control systems, like SCADA systems, with a focus on mitigations for published vulnerabilities.
- ICS Medical Advisories that focus on medical cybersecurity, including medical devices, with a focus on mitigations for published medical vulnerabilities.

Additionally, Health-ISAC serves as one of the primary security communications channels for the healthcare and public health sector regarding cyber threats. Health-ISAC analyzes member-provided incident reports/other intelligence and shares alerts and mitigation strategies with members and other partners/the sector, as appropriate.

Investigate and Declare a Cyber Incident

The medical product manufacturer should have clear processes in place to rapidly notify the Cyber Incident Response Manager (i.e., designated in the preparation phase), or another appropriate individual/team within the firm, of a cyber threat, and provide the response manager/responsible individual with the authority to identify, declare, and escalate a cyber incident.

Discerning actual security incidents from the many alerts and indicators can be a challenge. Intrusion detection systems may produce false positives, while employee reports of suspicious behavior may also not result in actual compromise.

Before engaging the CIRT Advisory/Leadership Group to convene the Full Cyber Incident Response Team, the Cyber Incident Response Manager may initially stand up a First Response Team who can accurately analyze and confirm an incident. This team primarily includes the Cyber Incident Response Manager and IT technical support staff.

The First Response Team can perform an initial analysis to determine which networks, systems, or applications are affected; the access vector and nature of any intrusions; and any known information about the root cause or threat actor behind the incident. This information will allow the incident response team to categorize and prioritize the incident and identify and take appropriate actions.

Incidents should not be handled on a first-come basis but rather prioritized based on safety impact, operational and functional impact, quality impact, information impact, and recoverability from the incident.

Operational and Functional Impact

Cyber incidents may impact the business and operational functionality provided by the IT and OT systems. The incident manager should consider how the incident will impact affected systems (including potential impacts to production output) not only in the immediate time frame but also looking ahead to the future if the incident is not immediately contained.

Quality Impact

Cyber incidents affecting the operational technology of medical product manufacturing process may impact the quality of medical products produced, stored, or otherwise managed. Actual or potential impacts to the quality of medical products will trigger processes to manage potentially adulterated products including investigating completed inventory for quality impacts, initiating regulatory and customer notifications, conducting recalls, and other actions.

Information Impact

Incidents may compromise sensitive and proprietary information (e.g., intellectual property or commercially sensitive information). The incident manager should consider how data exfiltration will not only affect the medical product manufacturer's overall mission but also that of partner organizations as well. Compromise of certain information may also implicate data related regulatory, statutory, or contractual requirements.

Recoverability from the Incident

The time and resource expenditure in handling and recovering from an incident is primarily dependent on the scale and nature of the incident. The Cyber Incident Response Team should carefully weigh the effort necessary to fully recover from an incident against the value the recovery effort will create.

Once an incident is confirmed, the Cyber Incident Response Manager should categorize the severity of the incident and engage the CIRT Advisory/Leadership Group to confirm the severity level and convene the full CIRT at the appropriate scale for incident severity as well as an estimate of the recovery efforts required. The CIRT should engage in investigative activities in coordination with the organization's legal counsel.

Engaging Help: Activating the Response Team and Engaging Resources

Activate the Cyber Incident Response Team

Once a cyber incident has been identified, the Cyber Incident Response Manager and Cyber Incident First Response Team should confirm the incident and work with the Advisory/Leadership Group to convene a full Cyber Incident Response Team including appropriate external parties.

The make-up of the CIRT will initially depend on the scale of the incident. A low-severity incident may require only the IT technical support team, public affairs, and legal representatives while the incident is contained and investigated. High-severity incidents may require immediately convening all representatives on the CIRT to begin standing up a round-the-clock incident response operation.

The medical product manufacturer's cyber incident response plan should outline the process to activate the response team and the logistics to support it. The CIRT should determine how frequently the team will meet and be briefed, how updates will be delivered (e.g., email, in-person meetings), and backup communication methods if the primary systems are affected by the cyber incident.

Consider designating and pre-staging the following for CIRT coordination:

- A dedicated operations center for central communication and coordination and a dedicated conference bridge for team members to meet.
- Encrypted messaging systems or other secure systems for incident communication.
- Mechanisms and procedures for backup communication tools in case usual systems are unavailable as a result of the cyber incident.
- Dedicated cell phone directory, in both digital and hard-copy form, for CIRT members for off-hour support and onsite communications.
- Printed copies of incident response procedures, contact lists, and incident handling forms.
- Secure storage facility for securing evidence and other sensitive materials.
- Secure file system, application, or database with access restrictions to store sensitive incident handling forms and information.

Engage Expert Response Resources

Few medical product manufacturers, regardless of size, can manage a significant cyber incident with in-house resources alone. Many medical product manufacturers employ third-party support staff to supplement in-house cybersecurity, monitoring, and response capabilities. When an incident requires expertise, tools, or capabilities beyond the resources of manufacturer staff, vendors of affected equipment and contracted cybersecurity service providers are often the first line of contact for cyber incident response, as their team may be equipped to help the manufacturer assess and respond to the threat.

In a major cyber incident, medical product manufacturers will likely need to engage a bevy of external response organizations: from law enforcement to information-sharing organizations and industry associations. In the case of a highly complex cyber incident or one that disrupts manufacturing, smaller to medium-sized medical product manufacturers may not possess the necessary expertise, staff capacity, or resources to effectively mitigate the incident.

See Section IX for further discussion of industry, regulatory, law enforcement, and other outside response entities that are important to cyber incident responses in the context of medical product manufacturers.


Take Action: Containment and Eradication

Conduct Initial Containment Actions

The Cyber Incident Response Manager and technical staff from the cybersecurity team will evaluate the incident and identify initial actions needed to contain the incident and prevent its spread while maintaining operational and physical safety. The team should conduct a full forensic investigation with the assistance of an expert forensic investigator, as appropriate, to determine the root cause of the incident and document exploit pathways before taking extensive mitigation actions. Containing the incident should focus on preventing further damage, such as further isolating and segmenting systems, or disconnecting affected devices from the internet to isolate a breach. Before taking any steps, the team should evaluate the unique context of their organization in considering

containment activities and assess how their actions could impact the investigation. Forensic evidence should be captured and preserved.

Figure 3. Example Do's and Don'ts During Initial Response



Some actions should not be taken unless or until instructed by the Incident Response Manager or other responsible designee. For example:

- **Do not shut down servers and systems** as this clears the temporary memory that can provide valuable information about the incident.
- **Do not shut off a server from the internet** as it may be difficult to determine the extent of compromise if the server is disconnected from its control server.
- **Do not restore affected systems from a backup** until the team can verify that backups have not been compromised.

During an incident response, you should take certain actions. For example:

- **Invoke previously documented processes** such as capturing and preserving forensic data (e.g., logs).
- **Start documenting the incident and all actions taken** with detailed notes and timeline.
- **Start preparing any external and internal communication** that may be required during the response.

Carefully Capture and Document Incident Information

According to organizational policies, begin recording detailed and precise information about a suspected incident immediately, and continue updating incident documentation throughout the response. The Cyber Incident Response Manager should coordinate with the team to gather the following information, which will help document the response (i.e., utilize documentation templates developed in the preparation phase) throughout the incident; brief the Full CIRT, Advisory/Leadership Group, and other appropriate parties; and conduct required reporting or other notification.

Crisis Communication

Secure internal communication channels with encrypted email and chat messaging capabilities may be used to direct internal actions and disseminate information on a need-to-know basis. The use of secure internal communication channels is dependent on the availability of those as the incident may impact an organization's communication capabilities.

Only some of these details will be shared with any given stakeholder. The information included in any reports to law enforcement or when complying with legal or regulatory reporting requirements will vary depending on the circumstances. Maintain incident information records using a secure application or database. Access to incident records should be restricted due to the sensitive nature of the data.

In that context, early involvement of legal counsel may provide attorney-client privilege for certain types of information and communications during cyber incident responses that may help an impacted firm prepare for or mitigate future legal actions. While communicating during the cyber incident, coordinate with appropriate the legal counsel to understand these considerations and put procedures in place to properly mark documentation and communications that are privileged.

What to Document

Note: Ensure all documents have appropriate headers, labels, and classifications, as needed (attorney-client privilege, PII, etc.).

1. Logs or other records of the incident, including:
 - Identification of Indicators of Compromise (IOCs); tactics, techniques, and procedures (TTPs), etc.
 - Preservation of forensic evidence.
2. Type of incident.
3. Date and time of the incident.
4. Status of the incident (Is it still ongoing?)
5. How the incident was discovered and the individuals who discovered it
6. Affected devices, applications or systems.
7. Current anticipated impacts of the incident, both inside and outside the organization, including impact on production volume and quality, including products already shipped.
8. The type and sensitivity of data stored in affected systems.
9. Any mitigation measures planned or already taken.
10. List of stakeholders already contacted or other resources engaged, including copies of communications with stakeholders (e.g., a vulnerability communication).
11. Details of the point-of-contact for the organization, incident response team point, and other parties involved in the response.
12. For incidents that exploit third party entities, maintain documentation related to that third party (technical information, contracts, communications, etc.).

Execute Evidence Gathering, Handling, and Preservation Procedures

The cyber incident IT support team should begin conducting a full forensic investigation according to organizational policies. This is necessary for the organization to understand the full nature and magnitude of an incident, identify pathways and actions of potential intruders, and determine how to completely remove the threat. Preserving, securing, and documenting evidence during this investigation is necessary for law enforcement to investigate and prosecute criminal attacks that steal sensitive data or malicious attacks that target healthcare operations.

The CIRT should meet with law enforcement agencies and legal staff to develop appropriate evidence-handling procedures in advance of an incident. Some organizations may contract with third-party entities that provide forensic investigation services for cyber incidents. The manufacturer can contact and request support or guidance on forensic investigation and documentation from partner organizations. Local, state, and federal law enforcement agencies can provide guidance on preserving evidence or even support onsite investigation in a severe incident.

See Section IV: Engaging Help for guidance on engaging federal and industry organizations during a cyber incident response.

Evidence Preservation Practices

Commonly recommended evidence-preservation practices in cyber incidents may include:

- Preserve affected system log files such as firewall, VPN, mail, network, client, web, server, antivirus, and intrusion detection system logs.
- Work with forensic experts to dynamically image all affected systems before disconnecting to preserve memory images, which can help identify sophisticated threat techniques that do not “write” to the hard drive. Memory images and logs are critical to identifying the origin of a threat and what data may have been accessed or lost.
- Avoid probing affected computers or systems unless directed by a forensic expert, as this could alter evidence or alert unauthorized actors that their activity has been detected, which might cause them to conceal their tracks or cause further system damage.
- Law enforcement agencies may request original hard drives as evidence, requiring the team to replace drives with a new system image.
- Store evidence and incident records in a secure, central location. Document how evidence was preserved and which individuals have handled all evidence throughout the incident.

Report the Incident as Required by Laws, Regulations, and Contracts

Manufacturers may be required to report an incident or intrusion to local, state, or federal entities—often within 72 hours or less of a manufacturer becoming reasonably aware that an incident has occurred—depending on the type of incident, the type of assets impacted, whether personal or proprietary data was exposed, or whether there is adulteration or other quality impacts to medical products.

While timely reporting is critical for compliance with cyber incident reporting statutory, regulatory, and contractual obligations, there are other benefits of early incident reporting and notifications. These include:

- Correlating incidents across the industry to identify coordinated incidents or incident trends. Reporting suspected or confirmed incidents to the Health-ISAC and other information sharing/analysis organizations early allows these partners to analyze the report against other reports and threat information, enabling early detection of a more coordinated, widespread incident.
- Mitigation measures and expertise. Organizations may be able to recommend mitigation steps for similar cyber incidents or conduct analysis of malware or threat signatures to identify ways to mitigate the incident.
- Incident investigation support. Several external response groups can support the manufacturer’s forensic analysis and investigation of an incident, either remotely or onsite.

- Ready response and coordination resources. Notifying external response groups early can help kickstart cross-industry coordination, prepare response teams for potentially severe incidents, and support messaging coordination among response partners.

Additionally, medical product manufacturers should consider several aspects when reporting cyber incidents. Items to consider include:

- Consult with legal counsel before making any notification outside of the manufacturer. Determine and authorize acceptable circumstances for notification in advance.
- Review information protections and ensure non-disclosure agreements, if appropriate, are in place before voluntarily sharing information. Review the protections offered by the ISACs and government agencies to understand how information will be protected.
- Identify what information about the incident can be shared with others.
- Designate liaisons to communicate with external response groups where possible to avoid overloading the Cyber Incident Response Manager. Prepare talking points in conjunction with legal, communications, and other CIRT members, and require liaisons to communicate only what is in the talking points.
- Identify contacts and build relationships with law enforcement in advance. Understand their expectations for information and access if the manufacturer reports a cyber crime, and how to coordinate with law enforcement during response and recovery.
- Disclose if you notify more than one law enforcement agency (e.g., FBI) or other government agency (e.g., CISA, HHS) to avoid jurisdictional or interagency conflicts. Track and share the case number and contact person assigned.

The sections below discuss and describe examples of these cyber incident reporting requirements relevant to medical product manufacturers. However, these only address relevant examples at the time of the publication of this document. Regulations and requirements may evolve over time to respond to the evolving cybersecurity threats/contexts of the sector including the development of new obligations important for medical product manufacturers to consider in their cyber incident preparedness and response.

Additionally, data breach and privacy-related reporting requirements (e.g., HIPAA, GDPR) may be relevant to some medical product manufacturers, but they are not discussed in this publication.

1. Federal Cyber Incident Reporting Obligations

Medical product manufacturers experiencing a cyber incident should be aware of multiple statutory and regulatory requirements to report the occurrence of cyber incidents and ransomware payments. These reporting requirements include in many cases, medical product manufacturers and have specific deadlines and information requirements that are important to consider in the cyber incident response process.

Cross-Sector Reporting Requirements

For one, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 requires that a “covered entity” report a “covered cyber incident” to the Cybersecurity and Infrastructure Security Agency (CISA) no later than 72 hours after the covered entity “reasonably believes that the covered cyber incident has occurred.” Additionally, “a covered entity

that makes a ransomware payment as the result of a ransomware attack against the covered entity shall report the payment to the Agency [CISA] not later than 24 hours after the ransom payment has been made.” CISA’s CIRCIA rule will describe the definition of a covered entity and other details of the reporting requirements.

Many medical product manufacturers may be required to report cyber incidents and ransomware payments under CIRCIA, either by the rule’s size criteria or sector-specific criteria. Even medical product manufacturers who are not a “covered entity” for the purposes of CIRCIA can submit voluntary reports of incidents through the CIRCIA reporting system.

Outside of CIRCIA, the Securities and Exchange Commission (SEC) maintains some requirements for cyber incident reporting. For example, public companies subject to the reporting requirements of the Securities Exchange Act of 1934 must report certain cyber incidents to the SEC via an 8-K form “within four business days after a registered public company determines that it has experienced a material cybersecurity incident.” Some medical product manufacturers, especially larger manufacturers, may be public companies required to report cyber incidents under the SEC rules.

Medical Product Regulatory Reporting Requirements

Beyond these cross-sector reporting requirements, medical product manufacturers must consider the reporting obligations of regulators—particularly, those of the U.S. Food and Drug Administration (FDA). FDA monitors the ongoing safety and effectiveness of medical products and takes action, as appropriate (e.g., issuing safety communications, requesting recalls, inspections of manufacturing facilities, and seizure of adulterated devices), to address any subsequent issues that arise with FDA-regulated manufacturers or products—including issues that arise from cyber incidents.

For example, in the medical device context, the Medical Device Reporting (MDR) regulation, 21 CFR part 803, contains mandatory requirements for device manufacturers, importers, and device user facilities to report certain device-related adverse events and product problems to the FDA. These can include adverse events, malfunction, and other medical issues that may result from a cyber incident impacting a device manufacturer.

FDA also requires the submission of reports of medical device corrections or removals (“voluntary recalls”) under 21 CFR part 806. Each device manufacturer or importer must submit a written report to the FDA on any correction or removal of a device(s) if it was initiated by such manufacturer or importer to reduce a risk to health posed by the device or to remedy a violation of the Federal Food, Drug, and Cosmetic Act caused by the device, which may present a risk to health. These reports must be submitted within 10 working days of the time the manufacturer or importer initiated the correction or removal. Medical product manufacturers experiencing a cyber incident impacting product quality, as described in Section III(a)(a), may need to pursue a recall and, therefore, should be aware of this reporting requirement under 21 CFR part 806.

Additionally, under section 506J of the Federal Food, Drug, and Cosmetics Act, during, or in advance of, a public health emergency, manufacturers of certain medical devices must notify the FDA of an interruption or permanent discontinuance in manufacturing. These devices include: 1) devices that are critical to public health during a public health emergency, including those that are life-supporting, life-sustaining, or intended for use in emergency medical care or during surgery; or 2) devices for which the FDA determines information on potential meaningful supply disruptions is needed during a public health emergency. This required notification must occur at least six months in

advance of a permanent discontinuance in manufacturing of a device or an interruption in manufacturing of a device that is likely to lead to a meaningful disruption in supply of the device in the United States.

Outside of medical devices, the FDA maintains required and voluntary reporting processes related to other FDA-regulated medical products. As part of the cyber incident response plan, a medical product manufacturer should familiarize itself with regulatory reporting requirements specific to the medical product types that it manufactures and jurisdictions in which it is to be governed, and complete that reporting, as appropriate, during a cyber incident.

International Reporting Requirements

While these examples of cyber incident reporting requirements describe obligations under statutes and regulations for medical products and their manufacturers in the United States, similar requirements exist outside of the United States. As a medical product manufacturer often has an international presence and medical products may be manufactured for sale outside of the U.S., it is important for a manufacturer to be aware of and act upon reporting obligations both in the U.S. and abroad during a cyber incident.

For example, a cyber incident causing interruption to the supply of a medical device within a European Union member state may be required to report such incident/interruption. Specifically, Regulation (EU) 2024/1860 requires that:

“where a manufacturer anticipates an interruption or a discontinuation of the supply of a device, other than a custom-made device, and where it is reasonably foreseeable that such interruption or discontinuation could result in serious harm or a risk of serious harm to patients or public health in one or more Member States, the manufacturer shall inform the competent authority of the Member State where it or its authorized representative is established, as well as the economic operators, health institutions and healthcare professionals to whom it directly supplies the device, of the anticipated interruption or discontinuation.”

2. Cyber Insurance Contract Requirements (if applicable)

Organizations may have purchased cyber insurance to help mitigate losses associated with a medical product manufacturing incident. If an organization has such a policy, it should ensure that it is responding consistently with the policy requirements.

Additionally, a manufacturer should engage the cyber insurance representative and review policies before responding to an incident, as policies may dictate certain response actions (e.g., using only approved incident response vendors, notifying law enforcement, or using prescribed evidence-gathering processes). The manufacturer should comply with insurance policy notice requirements to preserve the possibility of obtaining coverage for any losses associated with the incident. Furthermore, information needed to prepare and support a claim should be collected.

Develop Response Solutions and Assess Resource Needs

Once the incident is contained and a forensic investigation is complete, the organization should develop a plan to mitigate the incident, ensure the compromise has been eradicated, and restore systems to normal operations.

During this process, the medical product manufacturer should assess resource needs, including the type of expertise and the number of personnel required, hardware and software equipment needed, and replacement devices required, depending on the type of incident. The Incident Response Manager should work with senior management to authorize the use of external response partners as necessary to determine and implement mitigation actions.

Enact the Response Plan and Eradicate the Threat

Incident eradication should only be conducted after a complete investigation, and only by an experienced team of cybersecurity experts. The incident response leads should coordinate the closure of any exposed vulnerabilities and remove the compromise and any artifacts left by the incident (malicious code, data, etc.). This process should be rapid, thorough, synchronized, coordinated, and deconflicted to avoid giving potential unauthorized actors time to cover their tracks or enact further damage.

Eradication steps may include:

- Disabling breached user accounts and/or changing passwords.
- Updating network intrusion detection system signatures to assess indicators of similar attacks in other parts of the environment.
- Identify ongoing exfiltration of data using packet capture (i.e., pcap) to assess network traffic.
- Running a malware scanner to remove the compromised files or services.
- Closing all network vectors of exfiltration and potential vectors for re-infection.
- Informing employees of the incident or follow-up actions.
- Enabling additional monitoring/visibility, such as dark web monitoring.
- Coordinating with operational technology leads and engineers to appropriately eradicate threats and shutdown/restart manufacturing processes and associated affected systems.

Furthermore, sophisticated or severe incidents may require the support of federal and industry experts to support investigation, mitigation planning, and eradication. Section IV: Engaging Help provides an overview of how to engage these resources during a significant event.

Incident Recovery and Post Incident Activity

Recover from an Incident

Following the eradication of a cyber incident, medical product manufacturers should restore the system to return to normal operation and detect/remedy vulnerabilities to prevent similar incidents from occurring. There are multiple ways to restore a system after an incident, such as those described in the following table. Processes for restoration

will ultimately be dependent on the affected systems. For example, engineers and other manufacturing subject matter experts play a critical role in the safe and appropriate restoration of affected manufacturing systems.

Table 3. Examples Mechanisms for System Restoration

Remove the incident artifacts and replace any compromised files with clean versions.	<p>Pros: Fast recovery time; cost-effective</p> <p>Cons: Might leave undiscovered cyber threat artifacts behind</p>
Restore from a backup	<p>Pros: Moderate recovery time; cost-effective</p> <p>Cons: Only possible if backups are available, have been regularly updated, and/or known to be unaffected</p>
Rebuild the systems(s) or environment	<p>Pros: The only way to rectify the affected processes is if backups are not available and/or may be affected</p> <p>Cons: Slower recovery time; significant costs; possibility of data loss</p>

Conduct After-Action Review

At the conclusion of the incident response, management should receive an after-action report on the incident, the response, lessons learned, and any follow-on activities or recommendations including changes to the incident response plans and outside resources engaged. Additionally, medical product manufacturers should assess response activities to verify attack threat vectors are completely eradicated and ensure steps are taken to prevent similar attack incidents in the future. Potential post-incident actions include:

1. Internal Considerations and Actions

- Track metrics. Determine the status of impacts or recovery of the systems after the cyber incident by utilizing existing, ongoing metrics and data that measure security controls and the operations of a system within the medical product manufacturer. Potential metrics may include:
 - Elapsed time from the initiation of the incident to incident identification.
 - Elapsed time from incident identification to response of the First Response Team members to the incident.
 - Amount of labor time, financial resources, or other resources spent on the incident—including accountings by incident stage.
 - Strengthen security. Enhance system monitoring, administrative policies, and other protective measures to limit future risk of similar incidents and increase security.
 - Document findings. Record threat assessment, procedures, roles and responsibilities, metrics tracking, and process adjustments.
 - Update IR procedure and training. Based on lessons learned and findings of after-action review, make necessary updates to the Cyber Incident Response Plan, conduct additional training for

individuals involved in the response, and address other identified cyber incident preparedness needs.

- Refresh security training. Schedule re-training on relevant security protocols, send “refresher” emails to key employees on security guidelines, and identify additional training to prevent similar incidents in the future.
- Consider resource needs. Based on lessons learned and IR metrics, assess whether applied resources were adequate or if change or improvement is needed.

2. External Considerations and Actions

- Report mitigations. If deemed appropriate, in consultation with legal counsel, report the incident and subsequent response actions to the ISACs for industry situational awareness, in addition to required reporting to government and regulatory authorities.
- Notify partners that it is safe to reconnect. Consistent with organizational policies and appropriate status of recovery, suppliers and other partners connected to a medical product manufacturer network should be notified that connections can be restarted. For manufacturers with many connected partners, notifying an appropriate ISAC can be helpful to facilitate notification to many partners through one action.
- Continue regulatory compliance activities. For example, if a cyber incident impacted the quality of medical products and a recall was subsequently initiated, the continuation of compliance activities to recall products and address that situation would continue beyond the conclusion of the incident, as necessary.

Appendix A: Resource Matrix and Additional Resources

Matrix of Example Sector Resources

This matrix describes various types of resources and their associated activities, support actions, and coordination activities that medical product manufacturers may consider as part of the preparation for cyber incidents and cyber incident response activities.

Resource Type	Name/Description	Activities, Support Actions, & Coordination
Information Sharing and Analysis Center (ISAC)	Health-ISAC Healthcare cybersecurity information sharing and analysis organizations focus on providing information to their members as part of collaborative network of critical infrastructure entities in the healthcare and public health sector.	<ul style="list-style-type: none">• Provides timely, actionable, and relevant information on cyber threats, vulnerabilities, and incidents.• Convenes working groups, initiatives, education, and other activities for members and stakeholders (including medical product manufacturers) related to evolving healthcare cybersecurity topics and best practices.

Information Sharing and Analysis Center (ISAC)**Manufacturing-ISAC**

Manufacturing cybersecurity information sharing organization that focuses on providing information and tools to their members as part of a collaborative network of critical infrastructure entities in the manufacturing sector.

Federal Response**U.S. Food and Drug Administration (FDA)**

U.S. Department of Health and Human Resources (HHS)

Cybersecurity and Infrastructure Security Agency (CISA)

- Provides shared services and training opportunities for members related to healthcare cybersecurity topics.
- Provides timely, actionable, and relevant information on cyber threats, vulnerabilities, and incidents.
- Convenes discussion and meetings of ISAC staff, members, and other stakeholders related to evolving manufacturing cybersecurity threat topics and best practices.
- Provides shared services and training opportunities for members related to manufacturing cybersecurity topics.
- Works collaboratively to address and mitigate the impacts of cyber incidents including direct impacts to FDA-regulated products, indirect impacts in the form of disruptions to manufacturing and business operations, and shortage and supply chain impacts.
- Ensures compliance with statutory, regulatory, and other requirements for regulated medical as appropriate in the context of each cyber incident (e.g., reporting, recalls, quality management systems).
- Serves as the sector risk management agency (SRMA) for the healthcare and public health sector.
- Coordinates significant cyber incident responses through HHS's Administration for Strategic Preparedness and Response (ASPR) including utilization of ASPR's regional staff/resources and coordination of a variety of federal partners.
- Provides information on cyber threats to the healthcare and public health sector through the Health Sector Cybersecurity Coordinating Center (HC3).
- Develops cybersecurity best practices for entities across the sector such as through private-public partnerships (e.g., HSCC, 405(d) program).
- Receives reports of cyber incidents, both voluntary reports and those required under the Cyber Incident Reporting for

Industry Support

Healthcare Sector Coordinating Council (HSCC) Cybersecurity Working Group

HSCC Cybersecurity Working Group is a public-private partnership of more than 420 industry and government entities (at the time of this publication) working to address emerging and ongoing cybersecurity challenges to the health sector.

Law Enforcement

Local/State Law Enforcement Agencies

State and local law enforcement offices may have a cyber division that can offer expertise or guidance on documenting and preserving evidence for a forensic investigation.

FBI Field Offices

The FBI conducts cyber threat investigations; supports cyber prosecutions; and supplies, supports, and coordinates intelligence analysis with federal agencies and the intelligence community through the National Cyber Investigative Joint Task Force (NCIJTF).

Critical Infrastructure Act (CIRCA) regulation.

- Provides a variety of free cyber services from cyber hygiene to cyber resilience reviews and information on other available, non-federal services.
- Provides critical infrastructure partners with no-cost, basic and intermediate cyber incident response training for staff.
- Develops and publishes cybersecurity best practice resources tailored to the healthcare and public health sector through a variety of topical task groups.
- Shares information and convene meetings of members and stakeholders (including medical product manufacturers) related to evolving healthcare cybersecurity topics and best practices.
- Reports suspected cyber crime, including any illegal intrusion, attack, or espionage, or if sensitive data is hacked, stolen, or held ransom.
- Offers guidance on evidence gathering and handling procedures.
- Supports forensic investigation and evidence documentation.
- Investigates and prosecutes cyber crimes.
- Coordinates the investigation with other agencies.

Medical product manufacturers should consider building personal contacts with local law enforcement during steady-state, cyber incident preparation activities.

- Same as above, particularly for sophisticated or serious incidents targeting medical product manufacturers. State law enforcement may also escalate to the FBI.
- Cyber threat investigations and intelligence analysis to thwart significant threats.
- Contacts known targets of classified cyber threats and attacks.
- Investigates and law enforcement provides expertise for significant cyber incidents on healthcare and public health infrastructure.

-
- Coordinates with DHS and HHS to support incident response related to the affected entities.
-

Additional Cyber Incident Response Related Readings and Resources

The following are additional readings and links to resources that are relevant for cyber incident response in the context of medical product manufacturers:

The following are additional readings and links to resources that are relevant for cyber incident response in the context of medical product manufacturers:

- HHS: [Healthcare System Cybersecurity: Readiness and Response Considerations](#)
- HSCC: [Health Industry Cybersecurity – Coordinated Healthcare Incident Response Plan](#)
- HSCC: [Health Industry Cybersecurity – Matrix of Information Sharing Organizations \(HIC-MISO\)](#)
- HSCC: [Operational Continuity – Cyber Incident \(OCCI\)](#)
- NIST: [Cybersecurity Resources for Manufacturers](#)
- FEMA: [Planning Considerations for Cyber Incidents: Guidance for Emergency Managers](#)
- NIST: [Incident Response Recommendations and Consideration for Cybersecurity Risk Management: A CSF 2.0 Community Profile \[Initial Public Draft\]](#)
- CISA: [Critical Manufacturing Sector](#)
- WEF: [Building a Culture of Cyber Resilience in Manufacturing](#)
- NIST: [Implementing the Health Insurance Portability and Accountability Act \(HIPAA\) Security Rule: A Cybersecurity Resource Guide](#)

Acknowledgements

The Health Sector Coordinating Council (HSCC) expresses its gratitude to the many member representatives who worked on the Operational Technology Manufacturing Cybersecurity Task Group (“Task Group”) and contributed significant hours and thought leadership to the development of this resource.

Additionally, HSCC sincerely appreciates the American Public Power Association (APPA) for their support of this incident response playbook. Published in 2019, the Public Power Cyber Incident Response Playbook was developed by the Nexight Group with the technical support of APPA and its sector members and based upon work supported by the U.S. Department of Energy under Award Number DE-OE0000811. This work served as a valuable resource for entities in the public power sector related to cyber incident response. The Task Group recognized this prior effort and success, and that the public power playbook could serve as a useful foundation for our work in the healthcare and public health sector. In that context, APPA graciously supported the Task Group’s adaptation of the Public Power Cyber Incident Response Playbook for the context of medical product manufacturers.

Furthermore, in recognition of the efforts to adapt and build out the following cyber incident playbook for medical product manufacturers, we wish to thank:

Jessica Wilkerson

Task Group Co-Lead

U.S. Food and Drug Administration

Edison Alvarez

Task Group Co-Lead

Becton Dickinson

George Dimock

Task Group Co-Lead

Merck

Monroe J. Molesky

Publication & Content Lead

U.S. Food and Drug Administration

Michael Bellovin

Merck

Phil Englert

Health-ISAC

Chris Gates

Velentium

Lisa Gilbert

U.S. Food and Drug Administration

Bill Proffer

Leidos

Ryan Schreck

Merck

Matt Simkovic

Johnson & Johnson

Allison Snyder

Johnson & Johnson

Axel Wirth

MedCrypt

Morgan Shuey

HSCC Cybersecurity Working Group
Member Support Intern