DARKTRACE

Building an Incident Response Plan for Healthcare

Introduction

In today's digital healthcare landscape, cybersecurity incidents are an ever-present threat. From ransomware attacks to data breaches, healthcare organizations face a myriad of risks that can compromise patient care, expose sensitive information, and cause significant financial and reputational damage.

To effectively respond to and mitigate these threats, it's critical for healthcare providers to develop a comprehensive Incident Response Plan (IRP).

In this playbook we'll explore the key elements of building an IRP tailored for the healthcare sector, drawing from best practices and guidelines such as those outlined by the National Institute of Standards and Technology (NIST).

The healthcare industry is increasingly becoming a prime target for cyber-attacks, making the implementation of an effective IRP a critical necessity. With the wealth of sensitive Personal Health Information (PHI) at stake, a robust and well-thought-out IRP is not just a regulatory requirement but a fundamental component of healthcare operations.

The importance of incident response planning in healthcare

Healthcare organizations are prime targets for cybercriminals due to the wealth of sensitive data they maintain and their critical role in providing essential services. According to recent data from the HIPAA Journal, there were numerous data breaches affecting millions of healthcare records in recent years. With the frequency and sophistication of attacks on the rise, having a well-defined IRP is no longer optional — it's a necessity.

An IRP provides a systematic, coordinated approach for detecting, analyzing, and responding to cybersecurity incidents. It enables healthcare providers to act swiftly and decisively to contain threats, mitigate damage, and restore normal operations as quickly as possible. Without a solid plan in place, organizations risk fumbling their responses, potentially exacerbating the impact of incidents.

For the healthcare sector, the stakes are particularly high. Not only are there legal and regulatory requirements to safeguard PHI under regulations like the Health Insurance Portability and Accountability Act (HIPAA), but the potential impacts of a data breach can also include disruptions to patient care, financial losses, and significant reputational damage.

An IRP helps organizations respond swiftly and effectively to security incidents, minimizing damage, ensuring compliance with laws like HIPAA, and maintaining public trust.

Key components of an effective incident response plan

Developing a comprehensive IRP involves several critical steps and components, which can be broadly categorized as preparation, detection and analysis, containment, eradication, recovery, and post-incident activities.

01. Preparation

Preparation is the cornerstone of an effective IRP. It involves the identification and assessment of risks, as well as the establishment of policies, tools, and resources necessary for incident response.

Understanding potential threats and vulnerabilities is crucial for effective incident response planning.

Begin by identifying all critical assets, including hardware, software, networks, and data, and assess the risks associated with them. When looking for potential threats, make sure to check for internal, external, and third-party risks.

Create an incident response policy

Before diving into the specifics of an IRP, it's important to establish an overarching incident response policy. This policy should:

- Define what constitutes a security incident
- Outline roles and responsibilities for incident response
- Establish documentation and reporting requirements
- Provide a framework for classifying and prioritizing incidents

Start by drafting comprehensive policies that outline how to respond to various types of incidents. These documents should be clear, detailed, and accessible to all staff.

Ensure that they cover all aspects of the incident response lifecycle, from detection to post-incident review, such as:

- Data classification and handling
- Access controls and authentication (including multi-factor authentication)
- Network segmentation and firewall configuration
- Encryption standards for data at rest and in transit
- Mobile device and remote access security
- Third-party vendor risk management
- Employee security awareness training
- Social engineering and phishing prevention
- Incident reporting and escalation procedures
- Business continuity and disaster recovery

These policies and procedures will shape incident response playbooks, which include step-by-step response procedures, roles and responsibilities, communication templates, escalation criteria, regulatory reporting requirements, and evidence preservation guidelines.

Make sure to define clear communication channels and procedures for:

- Internal stakeholders (employees, executives, board members)
- Patients
- Regulators
- Law enforcement agencies
- Media and public relations

Establish a secure, out-of-band communication method for the incident response team (e.g., encrypted messaging app).

Establish relationships with external partners and pre-negotiate contracts with key service providers to ensure rapid response capabilities:

- Law enforcement agencies
- Regulatory bodies
- External forensics firms
- Legal counsel specializing in cybersecurity
- Public relations firms with crisis management experience
- Threat intelligence sharing organizations

Assemble an incident response team

Form a dedicated incident response team with clearly defined roles and responsibilities. This team should include individuals with the necessary skills and expertise to handle different types of incidents. Ensure 24/7 coverage and on-call procedures for the team.

For smaller organizations, this may be a central team. Larger healthcare systems may opt for a distributed model with multiple teams or a coordinating team that provides guidance. Consider creating specialized sub-teams for different types of incidents.

Key roles to consider include:

- Incident classification and reporting thresholds
- IT Security
- Legal/Compliance
- Operations
- Risk Management
- Public Relations/Communications
- Human Resources
- Customer Service
- Senior Management
- Board of Directors (for escalation and oversight)

Conduct training and testing

Regular training and testing are essential to ensure that the response team is prepared to handle real incidents.

Conduct tabletop exercises and simulated attacks to:

- Familiarize team members with the IRP
- Test the effectiveness of response strategies
- Identify areas for improvement
- Practice communication and decision-making under pressure

Involve senior management and board members in select exercises to ensure top-level buy-in and understanding of incident response processes.

02. Detection and analysis

The ability to detect and analyze threats swiftly is crucial. This phase involves the following components.

Monitoring systems: Implement robust monitoring tools and techniques to detect anomalies that may indicate a security incident. These systems should be capable of real-time alerts to enable rapid response.

- **Establish baseline behavior:** Create baseline profiles for normal system and user behavior to more easily identify deviations that could indicate a security incident.

Incident classification: Develop a framework for classifying incidents based on their severity and potential impact. This classification helps prioritize response efforts and allocate resources effectively. Create a tiered incident severity scale (e.g., Low, Medium, High, Critical) with clear definitions and response requirements for each level.

Incident reporting systems: Implement a streamlined process for employees, patients, and partners to report suspicious activities or potential incidents. This may include a 24/7 incident reporting hotline, an internal ticketing system, and an anonymous reporting channel for potential insider threats.

Threat intelligence: Use healthcare-specific threat intelligence feeds to stay informed about emerging threats and attack patterns, participate in information sharing organizations, and implement automated threat intelligence platforms to correlate external threat data with internal security events.

Regular security assessments: Perform frequent vulnerability scans and penetration tests, including network infrastructure, web applications and APIs, and third-party integrations.

Incident documentation: Maintain thorough records of all incidents, including time of occurrence, nature of the incident, and steps taken in response. This documentation is vital for post-incident analysis and compliance reporting.

03. Containment, eradication, and recovery

Once an incident is detected, the next steps involve containment, eradication, and recovery to prevent further damage and restore normal operations.

Containment strategies: Choose containment strategies based on the nature and severity of the incident. Immediate containment is crucial to prevent further damage. This can involve isolating affected systems, blocking malicious traffic, or disabling compromised accounts.

Assess the scope of the incident: Rapidly determine the extent of the breach or attack by identifying all affected systems and data, determining the number of impacted patients, assessing potential financial losses and regulatory implications, analyzing the attack vector and methodology used.

Short-term containment: Implement immediate actions to isolate affected systems and prevent the incident from spreading. This might include disconnecting systems from the network or blocking specific IP addresses.

Long-term containment: Develop a strategy for more sustainable containment, which may involve temporary fixes or workarounds that allow systems to operate securely while the issue is fully resolved.

Eradication: After containment, work on eliminating the root cause of the incident. This may involve removing malware, patching vulnerabilities, and addressing security weaknesses. Ensure that all affected systems are thoroughly cleaned and secured to prevent reinfection.

Recovery: Restore and validate system functionality. This includes recovering data from backups, reinstalling compromised systems, and ensuring that all systems are fully operational and secure before they are brought back online.

04. Post-incident activities

Post-incident activities are essential for learning from the incident and improving future responses. These activities provide an opportunity to reflect on the incident, evaluate the response efforts, and identify areas for improvement.

This phase should be conducted no more than two weeks following a cyber event to ensure that details are still fresh in the minds of the response team.

For healthcare organizations, the Lessons Learned phase is particularly important due to the sensitive nature of healthcare data and the potential for significant reputational and financial damage from cyber incidents.

Incident review: Conduct a thorough review of the incident, including what happened, how it was handled, and what could be improved. This debriefing should involve all relevant stakeholders to gather diverse perspectives.

- **Document lessons learned:** Create a formal "Lessons Learned" document that can be shared with relevant stakeholders and used to inform future incident response efforts. This document should include a summary of the incident, what went well in the response, areas of improvement, and action items for enhancing future incident response capabilities.

Reporting and communication: Preserve evidence and document all containment actions in detail for internal review and external requirements. Communicate the incident and the response to all relevant parties, potentially including authorities and regulatory bodies, law enforcement, and legal counsel. This may also include media and patients if their data was compromised.

Analyze regulatory compliance: For healthcare institutions, it's critical to review whether all regulatory requirements were met during the incident response. This includes assessing if breach notifications were made within required timeframes and if the proper authorities were notified.

Update policies and procedures: Based on the lessons learned, update your IRP and related policies to address any identified gaps or weaknesses. Continuous improvement is key to staying ahead of evolving threats.

Enhance training and awareness: In light of the recent incident, improve cybersecurity training programs for employees, especially because real-world examples from the incident can be particularly effective at illustrating the importance of security practices.

Review third-party relationships: If the incident involved or impacted any third-party vendors, review these relationships and consider whether additional security measures or contractual changes are needed.

Share information: Consider sharing anonymized information about the incident with industry peers through information sharing organizations. This collaborative approach can help strengthen the overall cybersecurity posture of the healthcare sector.

Key takeaways and resources

IRPs help healthcare organizations adopt best practices and standardized approaches to manage cybersecurity incidents effectively. Continuous improvement through post-incident analysis and learning is crucial to enhancing the security of healthcare systems and patient data.

A variety of NIST publications and CISA guidance are available to assist healthcare organizations in developing and enhancing their IRPs, ensuring they are well-equipped to handle the unique challenges of the healthcare sector:

- Cybersecurity Incident Response Plans: From the United States Department of Health and Human Services (HHS).
- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients: Also from HHS.

How Darktrace can help

Darktrace delivers a multi-layered approach to cyber resilience in a single cybersecurity platform, helping teams stay proactive with their incident response planning, encompassing all phases: preparation, detection and analysis, containment, eradication, recovery, and post-incident activities.

For preparation, Darktrace understands your organization's unique risk profile, including an AI-based risk scoring system based on your specific technologies, firewall configurations, human communications patterns, CVEs, and MITRE adversary techniques, as well as your attack surface. Learn more:

Darktrace / Proactive Exposure Management →

Darktrace / Attack Surface Management →

For detection, analysis, containment, and eradication, Darktrace brings unprecedented visibility, threat detection, investigation, and incident response to cloud, network, email systems, endpoints, identities, and Operational Technology (OT). Powered by multi-layered AI, Darktrace can identify known and unknown threats and autonomously respond at machine speed. Learn more:

Darktrace / CLOUD →

Darktrace / NETWORK →

Darktrace / EMAIL →

For recovery, Darktrace provides an AI-recovery and incident simulation engine that uplifts teams, optimizes incident response processes, and reduces the impact of active cyber-attacks using an understanding of your data. Learn more:

Darktrace / Incident Readiness & Recovery →

And forensics: Darktrace's offerings have been bolstered with the acquisition of Cado Security Ltd., which enables security teams to gain immediate access to forensic-level data in multi-cloud, container, serverless, SaaS, and on-premises environments. Learn more:

Darktrace / Forensic Acquisition & Investigation →

See Darktrace in action with a personalized meeting:

Request a demo →

About Darktrace

Darktrace is a global leader in AI for cybersecurity that keeps organizations ahead of the changing threat landscape every day. Founded in 2013 in Cambridge, UK, Darktrace provides the essential cybersecurity platform to protect organizations from unknown threats using AI that learns from each business in real-time. Darktrace's platform and services are supported by 2,400+ employees who protect nearly 10,000 customers globally. To learn more, visit http://www.darktrace.com.

North America: +1 (415) 229 9100 Europe: +44 (0) 1223 394 100 Asia-Pacific: +65 6804 5010 Latin America: +55 11 4949 7696

darktrace.com | info@darktrace.com