CISO Toolkit – Incident Management

A CISO-developed resource to empower your team.

Scroll down for links to Guidance Document(s) and Resources

The CISO-developed resource toolkit on Incident Management provides security teams with well-defined processes and procedures for effectively responding to security incidents. This toolkit guides CISOs in identifying, containing, investigating, and remediating security breaches to minimize their impact and ensure a swift return to normal operations.

Toolkit Summary

ESTIMATED LABOR COST SAVINGS: $25,875 - $51,750

(Based on a range between $75-$150 per hour for a single FTE)

Title	Document Format	Document Type
CISO Developed Guide to Incident Management	PDF	Primary Guidance Document
Anatomy of a Breach	PDF	Supplemental Resource
Incident Response Reference Architecture	PPTX	Template
Incident Response Reference Architecture Definitions	PPTX	Template
Computer Incident Response Plan	PPTX	Template
Incident Response Plan	DOCX	Template
Incident Response Checklist	DOCX	Template
Ransomware - Pay or Not Pay - Decision Framework	PPTX	Tool
Threat Matrix	XLSX	Tool

The Value of the Toolkit

The Incident Management Resource Toolkit is an indispensable asset for CISOs and their teams, offering the following key benefits:

- **Comprehensive Coverage:** Addresses all aspects of incident management, from planning and response to investigation and remediation.
- **Practical Usability:** Provides templates and checklists for developing incident response plans, conducting incident investigations, and communicating with stakeholders.
- **Enhanced Compliance:** Helps organizations meet regulatory requirements for incident response and notification.

- **Strategic Insights:** Guides on emerging incident management trends and challenges, such as ransomware attacks and supply chain disruptions.
- **Increased Collaboration:** Fosters alignment between IT teams, security teams, and business units, ensuring a coordinated response to incidents.

Download Entire Toolkit

Primary Guidance Document

CISO Developed Guide to Incident Management

CISO Developed Guide to BCDR and IR in the Cloud

Resources and Tools

Supplemental Resource - The Anatomy of a Breach

Template - Incident Response Reference Architecture

Template - Incident Response Reference Architecture Definitions

Template - Computer Incident Response Plan

Template - Incident Response Plan

Template - Incident Response Checklist

Tool - Ransomware - Pay or Not Pay - Decision Framework

Tool - Threat Matrix