CISO Toolkit – Ransomware

A CISO-developed resource to empower your team.

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

The CISO-developed resource toolkit on Ransomware offers CISOs and security teams essential resources for defending against and responding to ransomware attacks. This toolkit provides guidance on proactive defenses, backup systems, and incident response plans, enabling CISOs to mitigate the impact of ransomware attacks and protect critical data.

Toolkit Summary

ESTIMATED LABOR COST SAVINGS: $17,250 - $34,500

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

Title	Document Format	Document Type
CISO Developed Guide to Ransomware	PDF	Primary Guidance Document
Ransomware Preparedness Assessment	XLSX	Tool
Planning for a Ransomware Attack	DOCX	Tool
Ransomware - Pay or Not Pay - Decision Framework	PPTX	Tool

The Value of the Toolkit

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

- **Comprehensive Coverage:** Addresses all aspects of ransomware prevention, detection, and response.
- **Practical Usability:** Provides templates and checklists for assessing ransomware risks, implementing ransomware prevention controls, and responding to ransomware attacks.
- **Enhanced Compliance:** Helps organizations meet regulatory requirements for ransomware preparedness and response.
- **Strategic Insights:** Guides on emerging ransomware trends and challenges, such as ransomware-as-a-service and double extortion attacks.
- **Increased Collaboration:** Fosters alignment between IT teams, security teams, and business units, ensuring a coordinated response to ransomware attacks.

Download Entire Toolkit

Primary Guidance Document

CISO Developed Guide to Ransomware

Resources and Tools

Tool - Ransomware Preparedness Assessment

Tool - Planning for a Ransomware Attack

Tool - Ransomware - Pay or Not Pay - Decision Framework