ChecklistGuro

Cybersecurity Incident Response Plan Checklist

Preparation & Planning

Establishing foundational elements and processes before an incident occurs. Focuses on team setup, asset identification, and risk assessment.

Define Scope of the Incident Response Plan (Logistics Specific)

Write something...

Maximum acceptable downtime for critical logistics systems (hours)

Enter a number...

Primary Incident Response Team Lead Designation

- □ IT Security Manager
- □ Operations Manager
- □ Designated Incident Response Lead

Critical Logistics Systems to be included in the plan (select all that apply)

□ Warehouse Management System (WMS)

□ Transportation Management System (TMS)

□ GPS Tracking Systems

□ Driver Mobile Devices/Telematics

□ Electronic Logging Devices (ELDs)

□ Order Management System (OMS)

Asset Inventory List (Logistics Specific)

Upload File

Date of Last Incident Response Plan Review/Update

Enter date...

Define Roles and Responsibilities of Incident Response Team Members

Write something...

Detection & Analysis

Procedures for identifying, triaging, and analyzing potential cybersecurity incidents. Includes monitoring, alerting, and initial assessment.

Initial Incident Severity Level (Based on Initial Assessment)

□ Informational
□ Low
□ Medium
□ High
□ Critical

Detailed Description of the Suspicious Activity/Event

Write something...

Estimated Number of Systems Potentially Affected

Enter a number...

Potential Affected Systems/Assets (Check all that apply)

□ TMS (Transportation Management System)
□ WMS (Warehouse Management System)
□ GPS Tracking Devices
□ Driver Mobile Devices
□ EDI (Electronic Data Interchange) Systems
□ Network Infrastructure
□ Cloud Storage
□ Customer Data (PII)

Relevant Logs or Screen Captures (if available)

Upload File

Date of Initial Detection

Enter date...

Time of Initial Detection

Source System/Log Where Incident Was Detected

Write something...

Containment & Eradication

Steps to limit the scope of an incident and eliminate the threat. Addresses isolation, system shutdown, and malware removal.

Incident Containment Strategy

- □ Network Segmentation
- □ System Isolation
- □ Process Termination
- □ Data Backup/Snapshot
- □ Implement Firewall Rules

Affected Systems/Services to Isolate

- □ Warehouse Management System (WMS)
- □ Transportation Management System (TMS)
- □ GPS Tracking Devices
- □ EDI/API Connections
- □ Driver Mobile Devices
- □ Fleet Management Software
- □ Customer Relationship Management (CRM) - Logistics Data

Detailed Description of Isolation Procedures

Write something...

Number of affected systems/devices

Enter a number...

Evidence Preservation Strategy (e.g., disk imaging, memory dumps)

Write something...

Malware Removal Method

- □ Automated Scan & Removal
- □ Manual Removal
- □ System Rebuild
- □ Forensic Imaging & Analysis (for later review)

Recovery & Restoration

Actions to return affected systems and data to normal operation. Focuses on data restoration, system rebuilding, and verification.

Time to Recovery (RTO) Target

Enter a number...

Recovery Point Objective (RPO) Target

Enter a number...

Last Successful Data Backup Date

Enter date...

Estimated time to restore core logistics systems

Detailed Restoration Procedures for TMS (Transportation Management System)

Write something...

Detailed Restoration Procedures for WMS (Warehouse Management System)

Write something...

Verification steps to confirm data integrity after restoration

Write something...

Systems Requiring Prioritized Restoration

□ TMS
□ WMS
□ GPS Tracking Systems
□ Driver Communication Devices
□ EDI/API Integration Points

Post-Incident Activity

Activities performed after the incident is resolved. Includes lessons learned, plan updates, and communication.

Detailed Incident Timeline Review

Write something...

Lessons Learned - Identify Contributing Factors

□ Lack of Training
□ Outdated Software
□ Configuration Errors
□ Insufficient Monitoring
□ Third-Party Risk
□ Human Error
□ Other (Specify in Long Text)

Specific Recommendations for Improvement (Based on Lessons Learned)

Write something...

Estimated Financial Impact (USD)

Enter a number...

Date of Plan Update/Review

Enter date...

Summary of Changes Made to the Incident Response Plan

Write something...

Overall Effectiveness Rating (1-5, 5 being highest)

□ 1
□ 2
□ 3
□ 4
□ 5

Logistics-Specific Considerations

Specific actions and controls needed due to the unique aspects of logistics operations (e.g., tracking systems, GPS data, driver devices).

GPS Tracking System Vulnerability Assessment

Write something...

Critical Data Types at Risk (e.g., shipment manifests, route information, driver details)

□ Shipment Manifests
□ Route Information
□ Driver Details
□ Customer Data
□ Inventory Data
□ Other (Specify in Long Text)

Number of Driver Devices (e.g., smartphones, tablets) Managed

Enter a number...

Primary Method of Communication with Drivers During an Incident

□ Two-Way Radio
□ Mobile Phone
□ Messaging App (Specify)
□ Other (Specify in Long Text)

Potential Impact of Compromised Fleet Management Software

Write something...

Last Review of Third-Party Logistics Provider Cybersecurity Assessments

Enter date...

Types of Data Stored on Driver Devices (e.g., ELD data, delivery confirmations, route planning)

□ ELD Data

□ Delivery Confirmations

□ Route Planning

□ Customer Information

□ Other (Specify)

Contact Person for Immediate Issues Related to Fleet Management Systems

Write something...

Communication & Reporting

Procedures for internal and external communication throughout the incident response process. Includes stakeholder notification and regulatory reporting.

Incident Severity Level (Initial Assessment)

□ Informational

□ Low

□ Medium

□ High

□ Critical

Initial Incident Summary (for internal documentation)

Write something...

Primary Communication Method (Internal)

□ Email

□ Phone Call

□ Instant Messaging (e.g., Slack, Teams)

□ Dedicated Incident Response Platform

Legal Counsel Notification Required?

□ Yes

□ No

□ Pending Assessment

Estimated Number of Affected Systems/Locations (Initial)

Enter a number...

Date of Incident Report Submission

Enter date...

Time of Incident Report Submission

Which stakeholders need to be notified?

□ Executive Management

□ Legal Counsel

□ Public Relations

□ Insurance Provider

□ Law Enforcement

□ Customers

Summary of External Communication (if applicable)

Write something...