**IR Plan, Playbook and Policy**

Contents

[Introduction 3](#_heading=h.gjdgxs)

[Executive Summary 3](#_heading=h.30j0zll)

[Incident Response Playbook 4](#_heading=h.1fob9te)

[Escalation Triggers 8](#_heading=h.3znysh7)

[Stakeholder Communication 9](#_heading=h.2et92p0)

[Data Template 10](#_heading=h.tyjcwt)

[Slideshow Outline 11](#_heading=h.3dy6vkm)

[Policy Outline 1: Malware Outbreak Response 12](#_heading=h.1t3h5sf)

[Policy Outline 2: Data Breach Response 1](#_heading=h.4d34og8)2

[Policy Outline 3: Employee Termination Procedure 13](#_heading=h.2s8eyo1)

[Conclusion 14](#_heading=h.17dp8vu)

[References 14](#_heading=h.3rdcrjn)

## Introduction

In an era where digital threats are increasingly sophisticated, ransomware remains a formidable challenge for organizations. To counter this, our project introduces a robust set of policies aimed at strengthening Canadian Tire’s cybersecurity defenses. By leveraging the NIST 4-step incident response process and integrating a comprehensive ransomware playbook, we ensure that Canadian Tire is well-equipped to handle ransomware incidents swiftly and effectively. This initiative not only enhances the company’s resilience against cyber threats but also safeguards its reputation and operational integrity.

## Executive Summary

In today’s rapidly evolving digital landscape, the threat of ransomware poses a significant risk to organizations. To address this, our project presents a comprehensive policy set designed to fortify Canadian Tire’s cybersecurity posture. This initiative leverages the NIST 4-step incident response process and integrates a ransomware playbook to ensure robust and proactive defense mechanisms.

**Project Overview:** The project encompasses the creation of three detailed policy outlines, each meticulously crafted to align with the ransomware playbook processes. These policies are designed to be automatically enacted upon the initiation of the playbook, ensuring swift and effective responses to ransomware incidents.

**Policy Outlines:**

1. **Purpose and Importance:** Each policy begins with a clear statement of its overall purpose, emphasizing its critical role in safeguarding the organization’s digital assets. The importance of these policies from a security standpoint is underscored, highlighting the potential risks and impacts of ransomware attacks.
2. **Activities and Responsibilities:** The policies delineate specific activities that must be performed, detailing the frequency and responsible parties. This ensures that all stakeholders are aware of their roles and responsibilities in maintaining the organization’s cybersecurity defenses.
3. **Integration with Ransomware Playbook:** Each policy is closely tied to the ransomware playbook, outlining how the playbook will be utilized within the policy framework. This integration ensures a cohesive and coordinated approach to incident response.
4. **Consequences of Non-Compliance:** The policies clearly articulate the consequences of non-compliance for both individuals and the organization. This serves as a deterrent against negligence and underscores the importance of adherence to the established protocols.

**Why These Policies Matter:** The rationale behind each policy is thoroughly explained in an accompanying slideshow, which also details the consequences of non-compliance. This educational component is crucial in fostering a culture of security awareness and accountability within Canadian Tire.

## Incident Response Playbook

**Step 1:** Preparation

**1.1 Incident Response Policy and Plan**

* **Policy Document**: Canadian Tire’s Incident Response Policy outlines the procedures and responsibilities for handling cybersecurity incidents.
* **Incident Response Team (IRT)**: The Computer Security Incident Response Team (CSIRT) includes IT security personnel, legal advisors, PR representatives, and senior management.

**1.2 Communication Plan**

* **Internal Communication**: Establish a secure communication channel (e.g., encrypted email, secure messaging apps) and internal messaging systems (e.g., Microsoft Teams) for the CSIRT.
* **External Communication**: Pre-drafted statements for media, customers, and stakeholders. Legal team to handle regulatory notifications. Designated spokesperson (PR Specialist) to handle media and public inquiries.

**1.3 Tools and Resources**

* **Security Tools**: Antivirus software, endpoint detection and response (EDR) systems, and network monitoring tools.
* **Endpoint Detection and Response (EDR) tools:** CrowdStrike Falcon, Cynet 360
* **Incident Management System:** ServiceNow
* **Forensic Tools:** EnCase
* **Backup & Recovery Systems Solutions**: Regular backups stored offline and tested for integrity. Veeam Backup & Replication
* **Communication Channels:** Microsoft Teams, Secure Email
* **Incident Response Plan Document**: Stored in SharePoint

**1.4 Training and Awareness**

* **Employee Training**: Regular phishing simulation exercises and cybersecurity awareness training for all employees.
* **CSIRT Training**: Incident response drills and tabletop exercises for the CSIRT.

**Step 2:** Detection and Analysis

**Objective:**Detect and analyze potential incidents to determine their scope and impact.

**2.1 Detection**

* **Monitoring Systems**: Continuous monitoring of network traffic and system logs using SIEM (Security Information and Event Management) tools.
* **Indicators of Compromise (IoCs)**: Unusual file encryption activities, alerts from EDR software, unexpected system reboots, unusual network traffic patterns, and ransom notes notes or messages demanding payment appearing on systems.
* **Detection Methods:**
  + Intrusion Detection Systems (IDS): Snort
  + Security Information and Event Management (SIEM): Splunk
  + User Reports: Encourage employees to report suspicious activities.
* **Initial Detection**:

Detected by EDR software alerting on suspicious file encryption activity

**2.2 Analysis**

* **Initial Triage**: Determine the scope and impact of the ransomware attack on business operations. Identify affected systems and data.
* **Malware Analysis**: Determine the ransomware variant using threat intelligence feeds. Analyze the ransomware type to understand its behavior and potential decryption methods and assess the extent of the infection

**2.3 Documentation**

* **Incident Log**: Maintain a detailed log of all actions taken, findings including timestamps and personnel involved.
* Use a standardized incident report template.

**Step 3:** Containment, Eradication, and Recovery

**Objective:**Contain the incident, eradicate the threat, and recover from the incident.

**3.1 Containment**

* **Short-term Containment**: Isolate affected systems from the network to prevent further spread. Disable shared drives, network shares and affected user accounts. Notify all employees to avoid opening suspicious emails or files
* **Long-term Containment**: Apply patches and updates to all systems to close vulnerabilities. Block malicious IP addresses and domains. Implement network segmentation to limit the spread of ransomware.

**3.2 Eradication**

* **Remove Malware**: Use antivirus and anti-malware tools to remove the ransomware from affected systems.
* **System Clean-up**: Ensure all traces of the ransomware are eradicated from the network by conducting a thorough forensic analysis and a thorough scan of the network.

**3.3 Recovery**

* **Restore Systems**: Restore systems from clean backups. Verify the integrity of restored data.
* **Monitor Systems**: Continue to monitor systems for any signs of residual ransomware activity or any signs of reinfections.

**Step 4:** Post-Incident Activity

**Objective:**Conduct a thorough review of the incident and improve future response efforts.

**4.1 Lessons Learned**

* **Post-Incident Review**: Conduct post-incident review meeting with all stakeholders for a thorough review of the incident to identify what went well and what could be improved.
* **Update Policies**: Revise incident response policies and procedures based on the lessons learned.

**4.2 Reporting**

* **Internal Reporting**: Prepare a detailed incident report for senior management.
* **External Reporting**: Share relevant findings with external partners and regulatory bodies, if required.

**4.3 Communication**

* **Internal Communication**:
  + Regular updates to senior management and affected departments
  + Use secure communication channels to share sensitive information
* **External Communication**:
  + Public relations team to handle media inquiries
  + Notify customers if their data was compromised
  + Coordinate with law enforcement if necessary

**4.4 Documentation**

* **Incident Timeline**:
  + Document all actions taken during the incident response
  + Maintain a log of communications and decisions made
* **Evidence Collection**:
  + Preserve logs, files, and other evidence for forensic analysis
  + Ensure chain of custody is maintained for all collected evidence

**4.5 Follow-up Actions**

* **Employee Feedback**: Incorporate feedback from post-incident reviews into the plan.
* **Continuous Improvement**: Implement additional security measures to prevent future incidents. Implement improvements to the incident response plan and conduct regular reviews and updates. Provide additional training to employees based on identified weaknesses and cybersecurity best practices. Simulate ransomware attack scenarios to test the incident response plan.

**Company-Specific Information for Canadian Tire**

**Company Overview**

* **Name**: Canadian Tire Corporation, Limited
* **Industry**: Retail
* **Headquarters**: Toronto, Ontario, Canada
* **Number of Employees:** 13,000+
* **Annual Revenue:** CAD 14.53 billion (2023)
* **Key Assets**: Customer data, financial records, supply chain systems

**Incident Response Team Members**

* **CSIRT Lead**: John Doe, Chief Information Security Officer (CISO)
* **IT Security**: Jane Smith, IT Security Manager
* **Legal Advisor**: Mark Johnson, Legal Counsel
* **PR Representative**: Emily Davis, Public Relations Manager
* **Senior Management**: Robert Brown, CEO
* **External Forensics Expert:** CyberSec Solutions Inc.

**Contact Information**:

* + CSIRT Lead: john.doe@canadiantire.ca
  + IT Security Manager: jane.smith@canadiantire.ca
  + Legal Advisor: mark.johnson@canadiantire.ca
  + PR Specialist: emily.white@canadiantire.ca
  + External Forensics Expert: contact@cybersecsolutions.com

**Critical Systems and Data**

* **Customer Database**: Contains personal and financial information of customers.
* **Point of Sale (POS) Systems**: Used for transactions in retail stores.
* **Supply Chain Management System**: Manages inventory and logistics.

**Additional Information**

* **Ransomware Type:** LockBit 2.0
* **Ransom Demand:** CAD 1 million
* **Incident Date:** September 20, 2024
* **Affected Systems:** Point of Sale (POS) systems, Customer Database

### Escalation Triggers

1. **Systems Affected: Servers**
   * **Reasoning**: Servers are critical infrastructure components. Any incident affecting servers can lead to significant downtime, data loss, or security breaches.
   * **Escalation**: This would typically escalate to the **Senior Systems Administrator** or **IT Director**.
2. **Incident Severity: SEV 1 (Critical)**
   * **Reasoning**: A SEV 1 incident indicates a major disruption affecting multiple users or critical systems, requiring immediate attention.
   * **Escalation**: This would escalate to the **Incident Response Manager** and potentially the **Chief Information Security Officer (CISO)**.
3. **Data Breach Detected**
   * **Reasoning**: Data breaches involve unauthorized access to sensitive information, posing legal and reputational risks.
   * **Escalation**: This would escalate to the **Data Protection Officer (DPO)** and the **Legal Team**.
4. **Prolonged Incident Duration (e.g., > 4 hours)**
   * **Reasoning**: Extended incidents can indicate deeper issues and require additional resources or expertise to resolve.
   * **Escalation**: This would escalate to the **Incident Response Team Lead** and possibly the **Executive Management**.
5. **Multiple Systems Affected**
   * **Reasoning**: Incidents impacting multiple systems can indicate a widespread issue, potentially affecting business operations.
   * **Escalation**: This would escalate to the **Operations Manager** and the **Chief Technology Officer (CTO)**.

### Stakeholder Communication

1. **Internal Stakeholders: Senior Management**
   * **Information**: Overview of the incident, impact on business operations, and steps being taken to resolve it.
   * **Reasoning**: Senior management needs to understand the business impact and the response strategy to make informed decisions.
2. **Internal Stakeholders: IT Department**
   * **Information**: Technical details of the incident, affected systems, and mitigation steps.
   * **Reasoning**: The IT department needs detailed information to effectively manage and resolve the incident.
3. **External Stakeholders: Customers**
   * **Information**: Brief explanation of the incident, its impact on services, and expected resolution time.
   * **Reasoning**: Keeping customers informed helps maintain trust and manage expectations.
4. **External Stakeholders: Regulatory Bodies**
   * **Information**: Detailed report of the incident, including data affected, response actions, and compliance measures.
   * **Reasoning**: Regulatory bodies require this information to ensure compliance with legal and industry standards.
5. **External Stakeholders: Vendors/Partners**
   * **Information**: Impact of the incident on shared systems or services, and any actions they need to take.
   * **Reasoning**: Vendors and partners need to be aware of incidents that could affect their operations or require their assistance.

**Information to Avoid Communicating**

* **Sensitive Internal Details**: Avoid sharing detailed internal processes or vulnerabilities that could be exploited.
* **Unverified Information**: Ensure all communicated information is verified to avoid misinformation.
* **Speculative Statements**: Stick to facts and avoid speculation about the cause or impact of the incident.

### Data Template

| **Data Name** | **Content** | **Rationale** |
| --- | --- | --- |
| Company Information |  |  |
| Company Name |  |  |
| Contact Title (Position) |  |  |
| Contact Availability |  |  |
| Contact data permissions (TLP) |  |  |
| Incident Info: |  |  |
| Incident Name |  |  |
| Incident Type |  |  |
| C Effect |  |  |
| I Effect |  |  |
| A Effect |  |  |
| Team Members (CSIRT) |  |  |
| Internal Stakeholders |  |  |
| External Stakeholders |  |  |
| Company data classifications & prioritizations |  |  |
| Categories of assets/devices that may be compromised |  |  |
| Measurable metrics that would indicate the playbook has been completed and closed |  |  |
| Reports that would need to be written and to whom and when |  |  |
| Frequency at which the Playbook needs to be tested and re-evaluated |  |  |

## Slideshow Outline

1. **Introduction**
   * Purpose of the policy set
   * Importance of having these policies
2. **Policy 1: Malware Outbreak Response**
   * Why this policy is recommended
   * Consequences of non-compliance
3. **Policy 2: Data Breach Response**
   * Why this policy is recommended
   * Consequences of non-compliance
4. **Policy 3: Employee Termination Procedure**
   * Why this policy is recommended
   * Consequences of non-compliance

## Policy Outline 1: Malware Outbreak Response

**Purpose:** To establish a protocol for responding to malware outbreaks within the company network.

**Importance:** This policy is crucial for maintaining the integrity and security of the company’s IT infrastructure, preventing data loss, and minimizing downtime.

**Activities:**

* **Detection:** IT staff must monitor network traffic and system logs daily for signs of malware.
* **Analysis:** Upon detection, the incident response team must analyze the malware to understand its behavior and impact.
* **Containment:** Immediate steps must be taken to isolate affected systems to prevent the spread of malware.
* **Eradication:** Remove the malware from all affected systems and apply necessary patches.
* **Recovery:** Restore systems from clean backups and monitor for any signs of reinfection.
* **Post-Incident Review:** Conduct a review to understand the root cause and improve future responses.

**Related Playbook:**

* **Malware Response Playbook:** This playbook provides detailed steps for detecting, analyzing, containing, eradicating, and recovering from malware incidents.

**Consequences of Non-Compliance:**

* **Individual:** Disciplinary action, up to and including termination.
* **Company:** Increased risk of data breaches, financial loss, and reputational damage.

## Policy Outline 2: Data Breach Response

**Purpose:** To outline the steps to be taken in the event of a data breach involving Personally Identifiable Information (PII).

**Importance:** Protecting PII is critical to maintaining customer trust and complying with legal and regulatory requirements.

**Activities:**

* **Detection:** Regular audits and monitoring to detect unauthorized access to PII.
* **Analysis:** Assess the scope and impact of the breach.
* **Containment:** Secure compromised systems and prevent further unauthorized access.
* **Notification:** Inform affected individuals and relevant authorities as required by law.
* **Eradication:** Remove any malicious actors or software from the network.
* **Recovery:** Implement measures to prevent future breaches and restore affected services.
* **Post-Incident Review:** Analyze the incident to improve security measures.

**Related Playbook:**

* **Data Breach Response Playbook:** This playbook details the steps for detecting, analyzing, containing, notifying, eradicating, and recovering from data breaches.

**Consequences of Non-Compliance:**

* **Individual:** Legal action and potential fines.
* **Company:** Legal penalties, loss of customer trust, and significant financial impact.

## Policy Outline 3: Employee Termination Procedure

**Purpose:** To ensure secure and efficient handling of IT resources when an employee is terminated.

**Importance:** Proper handling of IT resources during termination is essential to prevent unauthorized access and data breaches.

**Activities:**

* **Notification:** HR must inform IT of the termination at least 24 hours in advance.
* **Access Revocation:** IT must revoke all access rights and retrieve company-owned devices immediately upon termination.
* **Data Backup:** Ensure all critical data is backed up before disabling accounts.
* **System Monitoring:** Monitor systems for any unusual activity post-termination.
* **Exit Interview:** Conduct an exit interview to ensure all company property is returned and to address any security concerns.

**Related Playbook:**

* **Employee Termination Playbook:** This playbook provides detailed steps for revoking access, retrieving devices, and securing data during employee termination.

**Consequences of Non-Compliance:**

* **Individual:** Potential legal action for unauthorized access or data theft.
* **Company:** Risk of data breaches, financial loss, and reputational damage.

## Conclusion

By implementing these policies, Canadian Tire is taking a proactive stance against ransomware threats. The alignment with the NIST 4-step incident response process and the integration of the ransomware playbook ensure that the organization is well-prepared to detect, respond to, and recover from ransomware incidents. This project not only enhances the company’s cybersecurity resilience but also protects its reputation and operational integrity.

## References

Government of Canada, Public Services and Procurement Canada, Integrated Services Branch, Government Information Services, Publishing and Depository Services. (2013b, April 3). *Ransomware playbook.: D97-4/00-099-2021E-PDF - Government of Canada Publications - Canada.ca*. https://publications.gc.ca/site/eng/9.904133/publication.html?wbdisable=true

Canada, C. S. E. (2022, January 13). *Ransomware playbook (ITSM.00.099) - Canadian Centre for Cyber Security*. Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/guidance/ransomware-playbook-itsm00099

*How to draft an incident response policy | Infosec*. (n.d.). https://www.infosecinstitute.com/resources/incident-response-resources/draft-incident-response-policy/

*A guide to incident response plans, playbooks, and policy | CISO Collective*. (2023, May 2). Fortinet Blog. https://www.fortinet.com/blog/ciso-collective/incident-response-plans-playbooks-policy

CrowdStrike. (2024, July 11). *Incident Response Plan: Frameworks and steps - CrowdStrike*. crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/incident-response/incident-response-steps/

*Incident Response: What it is, Process and Examples*. (2023, November 26). https://www.threatintelligence.com/blog/incident-response

Murstad, F. (2024, September 10). *Incident Handler’s Handbook | SANS Institute*. https://www.sans.org/white-papers/33901/

*Information Security Policy Templates | SANS Institute*. (n.d.). https://www.sans.org/information-security-policy/

Cichonski, P., Millar, T., Grance, T., Scarfone, K., National Institute of Standards and Technology, United States Computer Emergency Readiness Team, & Scarfone Cybersecurity. (2012). Computer Security Incident Handling Guide. In *NIST Special Publication 800-61* (Revision 2). https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

ZCySec, T. (2024, July 13). What is NIST Incident Response Plan? NIST SP 800-61 S Computer Security Incident Handling Plan Guide 2024. *Z Cybersecurity*. https://zcybersecurity.com/nist-incident-response-plan-playbook/

Atlassian. (n.d.). *Get to know the incident response lifecycle | Atlassian*. https://www.atlassian.com/incident-management/incident-response/lifecycle#incident-response-lifecycle

Exabeam. (2024, June 16). *NIST Incident Response: 4-Step Process and Critical Best Practices | Exabeam*. https://www.exabeam.com/explainers/incident-response/nist-incident-response-4-step-process-and-critical-best-practices/

Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce. (n.d.). *Incident Response | CSRC | CSRC*. https://csrc.nist.gov/projects/incident-response

Government of Canada, Innovation, Science and Economic Development Canada, Office of the Deputy Minister, Digital Transformation Service Sector & Digital Transformation Service Sector. (2021, December 8). *Develop an Incident Response Plan: Fillable template and example*. https://ised-isde.canada.ca/site/cybersecure-canada/en/certification-tools/develop-incident-response-plan-fillable-template-and-example