**IR Plan, Playbook, and Policy**

For Canadian Tire Corporation

****

**By: Sukhvir Sahota**

TABLE OF CONTENTS

[**EXECUTIVE SUMMARY**](#_904t4bt3ey8v) **2**

[**INTRODUCTION**](#_9occnlmwzsd0) **3**

[Purpose](#_kndvuzzgxect) 3

[**POLICIES**](#_ypdbu5h1hx37) **4**

[**INCIDENT RESPONSE PLAN**](#_cy5iliq0u7y9) **11**

[Testing and Review Cycle](#_tfllic68cbck) 11

[Authority](#_uqmmht82i90i) 11

[How to Recognize a Cyber Incident](#_lgok40io6dx5) 12

[Cyber Security Incident Response Team](#_gtudrqm9iplt) 13

[CSIRT Responsibilities](#_i8bwhla1xmi8) 14

[Executives](#_dwog82xakg3o) 14

[Incident Handler](#_wdz5rpiiv3dg) 15

[Communications Expert](#_t9nx11uepsjd) 15

[CSIRT Team](#_juqjlfh4vcyo) 16

[Incident Type and Severity Matrix](#_o5ipq63i145e) 17

[Incident Response Framework](#_5jtcccb671f1) 18

[**RANSOMWARE INCIDENT RESPONSE PLAYBOOK**](#_40c5qivn9nwq) **20**

[Preparation](#_c5grejvqz1e2) 20

[Identification](#_2xyfkl6qxbsl) 20

[Containment](#_3t29p2lbgb6x) 21

[Eradication](#_hklkgjc5yna4) 21

[Recovery](#_nmiv9nxznvc2) 21

[Lessons Learned](#_64v5wy35jpdo) 22

[**CONCLUSION**](#_vjd934dpbts3) **22**

[**Appendix A: CSIRT Team Contact Information**](#_ngdk95l4tkk7) **23**

[External Contacts](#_1o0va6ry63aw) 24

[**Appendix B: Stakeholder Communications**](#_czv3d2fln5l4) **25**

[**REFERENCES**](#_co89m1454qh) **26**

# 

# 

# 

# EXECUTIVE SUMMARY

Cyberattacks are a constant threat, and *Canadian Tire Corporation* recognizes the importance of being prepared. These documents establish a comprehensive framework to manage and mitigate cyber incidents effectively, minimizing damage and safeguarding critical systems, customer information, and business operations.

In this report, we focused on the Incident response policies, plans, and framework, along with the playbook procedure for ransomware attacks. In the first part we focused on Canadian Tire's incident policy underscores the crucial roles and responsibilities delineated within its five key incident response policies: Endpoint Protection, Vulnerability Management, Risk Management, Business Continuity and Disaster Recovery, and Training and Awareness. These policies collectively aim to protect the organization's information resources, mitigate risks associated with cyber threats, ensure compliance with regulations, and promote a culture of security awareness among personnel.

In the Incident response plan process, Canadian Tire has developed a robust plan to address cyber incidents, particularly focusing on ransomware attacks. Regular testing ensures the plan's effectiveness, while clear roles and responsibilities have been assigned to key personnel. Recognizing the signs of a ransomware attack, such as system access issues and data anomalies, enables swift identification and response. The plan outlines a structured approach, including preparation, identification, containment, eradication, recovery, and lessons learned phases, ensuring a comprehensive response to incidents. By prioritizing cybersecurity readiness and continuous improvement, Canadian Tire aims to safeguard its operations and customer data against evolving cyber threats, maintaining trust and resilience in the digital age.

# INTRODUCTION

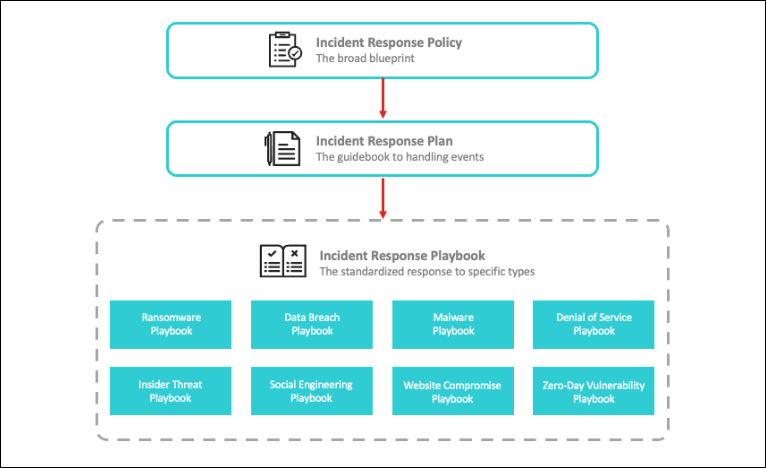
[Canadian Tire Corporation](https://corp.canadiantire.ca/English/about-us/default.aspx) (CTC) is a large, multi-divisional retail holding company in Canada. It operates over 1,700 stores across various brands (Canadian Tire, Mark's, Sport Chek, etc.) and employs a vast workforce. CTC operates within the retail industry, primarily selling merchandise and related services to consumers. Due to its size and structure, CTC has a diverse range of stakeholders with varying interests.

In today's digital world, cyberattacks are a constant threat. No organization, including Canadian Tire (CTC), is immune to these ever-increasingly frequent and sophisticated attacks. To safeguard our critical systems, customer information, and business operations, CTC has developed this comprehensive Incident Response (IR) Plan.

### 

### Purpose

In this report, we will be discussing the policies, Incidence response plan, and Playbook for the Randoswmehrre attack specifically associated with Candian Tire Corporation.



[The incident response policy](https://www.fortinet.com/blog/ciso-collective/incident-response-plans-playbooks-policy#:~:text=for%20an%20organization.-,Why%20Do%20We%20Need%20an%20Incident%20Response%20Policy%3F,incident%20response%20for%20the%20organization.) is the foundational document of any incident response team. It should act as a blueprint for incident response throughout the organization. Like any policy, this document sets the rules and governance around incident response for the organization. Unlike the other IR documents, the policy should be broad and not change much, if at all.

An Incident Response Plan exists to ensure Canadian Tire is prepared to manage cyber incidents effectively and efficiently comprehensive incident response plan is not just an option but a necessity for Canadian Tire in today's digital landscape. It helps the company mitigate the damaging effects of cyberattacks, improve preparedness, maintain compliance with regulations, and ultimately safeguard customer trust and brand reputation.

# POLICIES

[The incident policy](https://sprinto.com/blog/incident-management-policy/#:~:text=The%20incident%20policy%20defines%20the,seamless%20management%20and%20timely%20resolution)) defines the roles and responsibilities of different teams and individuals in managing and mitigating the incident efficiently. In this report, we are talking about the 5 incident response policies.

1. Endpoint Protection (Anti-Virus & Malware)
2. Vulnerability management policy
3. Risk management policy
4. Business continuity and disaster recovery policy
5. Training and awareness policy

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties. Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal.

| **Endpoint Protection Policy** | |
| --- | --- |
| ***Purpose*** | The Endpoint Protection Policy outlined in the Canadian Tire example has two main purposes:  **Protecting Information Resources:** This policy aims to safeguard Canadian Tire's information resources (data, systems, networks) from various cyber threats like viruses, malware, ransomware, and unauthorized access. By mandating approved endpoint protection software and email security measures, the policy helps prevent these threats from infiltrating the network and potentially compromising sensitive data.  **Ensuring Compliance:** The policy might also be driven by the need to comply with industry regulations or internal security best practices. For instance, some regulations mandate specific security controls for handling sensitive data. This policy ensures Canadian Tire adheres to such regulations by requiring approved security software and configurations. |
| ***Responsibilities*** | The responsibility for implementing and enforcing policies regarding information security typically falls within the purview of the IT department, often overseen by the Chief Information Officer (CIO) or Chief Information Security Officer (CISO). |
| ***Policy*** | * All Information Resources owned or managed by Canadian Tire must employ endpoint protection software and configurations approved by Canadian Tire's IT management. * Before connecting any non-Canadian Tire owned workstations or laptops to a Canadian Tire Information Resource, they must utilize endpoint protection software and configurations approved by Canadian Tire's IT management. * The endpoint protection software must remain unaltered, un-bypassed, and enabled at all times. * Each email gateway within Canadian Tire must utilize email virus protection software approved by Canadian Tire's IT management, following Canadian Tire's rules for setup and usage, including comprehensive scanning of all inbound and outbound emails. * Measures to prevent or identify the use of known or suspected malicious websites must be implemented. * All files received via networks or external storage devices must undergo malware scanning before use. * Any virus not automatically remediated by the virus protection software constitutes a security incident and must be promptly reported to Canadian Tire's IT Support.   Reference controls: SP 800-53 Rev. 5: AC-17, AC-11, CM-3, AC-18, SC-7 |
| ***Compliance and Consequences*** | * Non-compliance with the policy increases the risk of security breaches. * Inadequate endpoint protection increases the likelihood of data loss or theft, potentially exposing sensitive customer information, proprietary data, or confidential business records. * Canadian Tire may face legal consequences, including lawsuits, regulatory investigations, and civil liabilities if non-compliance with the endpoint protection policy results in harm to individuals or organizations. |
| ***Policy Review and Modification*** | The endpoint protection policy should be reviewed and modified at least annually, with additional reviews triggered by significant organizational changes, regulatory updates, technology advancements, incident analysis, stakeholder feedback, and ongoing training initiatives. |

| **Vulnerability management policy** | |
| --- | --- |
| ***Purpose*** | The purpose of Candian Tire’s Vulnerability Management Policy is to establish the rules for the review, evaluation, application, and verification of system updates to mitigate vulnerabilities in the IT environment and the risks associated with them. |
| ***Responsibilities*** | The Canadian Tire IT and CSIRT team holds overall responsibility for patch management implementation, operations, and procedures. It is often led by the Chief Information Security Officer (CISO) |
| ***Policy*** | This policy is more focused on  **Patch Management:**   * Routine scans of all Information Resources must be conducted to identify missing updates. * Missing software updates will be evaluated based on the risk they pose to Canadian Tire. * Updates posing an unacceptable risk must be implemented within a timeframe aligned with Canadian Tire's Vulnerability Management Standard. * Software updates and configuration changes applied to Information Resources must undergo testing prior to widespread implementation, following Canadian Tire's Change Control Policy.   **Penetration Testing:**   * Annual [penetration testing](https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/) of internal and external networks, as well as hosted applications, is mandatory for Canadian Tire. * Any exploitable vulnerabilities identified during a penetration test will be addressed and re-tested for verification.   Reference controls: SP 800-53 Rev. 5: CM-2, CA-7, CA-8 |
| ***Compliance and Consequences*** | Failure to comply may result in increased risk of security breaches, data loss or theft, operational disruptions, regulatory violations, reputational damage, and legal consequences. |
| ***Policy Review and Modification*** | These policies mandate routine scans for missing updates, evaluation of update risks, timely implementation of critical updates, testing of software changes, and annual penetration testing to identify and address vulnerabilities in internal and external networks and hosted applications. |

| **Risk management policy** | |
| --- | --- |
| ***Purpose*** | The purpose of the Risk Management Policy at Canadian Tire is to establish procedures for comprehensively assessing, treating, communicating, monitoring, and reviewing risks associated with information assets and operations. The policy aims to evaluate risks based on factors such as the strategic importance of business processes and information assets, their criticality to operations, legal and regulatory compliance requirements, operational significance, and stakeholder expectations |
| ***Responsibilities*** | The Chief Information Security Officer (CISO) or an equivalent executive typically holds primary responsibility for developing, implementing, and overseeing the Risk Management Policy at Canadian Tire. |
| ***Policy*** | * Risk assessments must comprehensively address administrative, physical, and technical risks associated with Canadian Tire's information assets and operations. * Information security risk management procedures must be established and encompass the following components, at a minimum:   + Risk Assessment   + Risk Treatment   + Risk Communication   + Risk Monitoring and Review * Risk evaluation criteria should be established to assess Canadian Tire's information security risks, considering the following factors:   + The strategic importance of the business processes and information assets involved.   + The criticality of the information assets to Canadian Tire's operations.   + Compliance with legal and regulatory requirements, as well as contractual obligations.   + The operational and business significance of ensuring availability, confidentiality, and integrity.   + Stakeholders' expectations and perceptions, along with potential negative impacts on goodwill and reputation.   Reference controls: SP 800-53 Rev. 5: Ac17, CA-6,7, SI-2, SI-5 |
| ***Compliance and Consequences*** | Non-compliance with risk management policies at Canadian Tire may lead to regulatory penalties, operational disruptions, financial losses, and reputational damage. |
| ***Policy Review and Modification*** | * Formal organization-wide risk assessments will be conducted by Canadian Tire no less than annually or upon significant changes to the organization's operations. * Canadian Tire reserves the right to take legal action against individuals or entities responsible for significant breaches of this policy, especially if the violation results in harm, financial loss, or legal liability for the organization. |

| **Business continuity and disaster recovery policy** | |
| --- | --- |
| ***Purpose*** | The Business Continuity and Disaster Recovery (BC/DR) policy serves two main purposes within an organization:  ***Ensuring Business Continuity During Disruptions***: By focusing on minimizing downtime, Protecting critical data and processes, and having Swift Recovery.  ***Protecting the Organization's Reputation and Well-being:*** By minimizing reputational damage and maintaining financial stability |
| ***Responsibilities*** | The responsibility for the Business Continuity and Disaster Recovery Policy at Canadian Tire typically falls on the Chief Information Officer (CIO), and Chief Information Security Officer (CISO). Additionally, collaboration with relevant stakeholders from IT, operations, security, and other departments may be necessary to ensure the policy's effectiveness and integration with overall business continuity and risk management strategies. |
| ***Policy*** | Canadian Tire prioritizes sustaining critical business processes during and after disruptions by implementing a [Business Continuity Plan (BCP)](https://www.newrocket.com/articles/planning-for-the-unexpected-with-business-continuity-management).  The BCP must include   * The BCP undergoes periodic testing and updates, with results shared with executive management. * Safety and security of personnel remain paramount, managed through an established structure and documented procedures. * The BCP includes risk assessments, critical systems inventory, supply chain identification, communication strategies, mitigation measures, and contingency plans for various disruption   Business continuity planning should ensure that:   * the safety and security of personnel is the first priority; * an adequate management structure is in place to prepare for, mitigate, and respond to a disruptive event using personnel with the necessary authority, experience, and competence; * documented plans, response, and recovery procedures are developed and approved, detailing how the organization will manage a disruptive event.   Reference controls: SP 800-53 Rev. 5: Ac17, CA-6,7, SI-2, SI-5 |
| ***Compliance and Consequences*** | Compliance with regulatory requirements, such as those outlined by regulatory bodies like the Canadian Securities Administrators (CSA) and industry-specific standards like [ISO 22301](https://www.iso.org/publication/PUB100442.html), is crucial to avoid fines, penalties, or legal action.  Failure to implement effective Business Continuity and Disaster Recovery measures may result in operational disruptions, data loss, financial losses, reputational damage, and erosion of stakeholder confidence, impacting Canadian Tire's ability to sustain critical business operations and compete effectively in the market. |
| ***Policy Review and Modification*** | Skipping the BC/DR plan at Canadian Tire risks financial blows from downtime and recovery costs. Even worse, frustrated customers and negative press could damage their reputation. Following the plan ensures smoother sailing during disruptions. |

| **Training and awareness policy** | |
| --- | --- |
| ***Purpose*** | Canadian Tire's training and awareness policy aims to achieve two key goals:  **Empower New Personnel**: By requiring security awareness training before accessing information resources, Canadian Tire ensures new employees (including contractors) understand how to protect sensitive data and prevent security breaches.  **Promote Security Awareness**: Canadian Tire requires all personnel to acknowledge information security policies. This reinforces a culture of security awareness and ensures everyone understands their role in safeguarding company information. |
| ***Responsibilities*** | The Chief Information Security Officer (CISO) or designated Information Security Officer (ISO) is responsible for the ownership, review, and updates of this policy. |
| ***Policy*** | * All new personnel must complete an approved Security Awareness training program prior to, or within 30 days of, being granted access to any Canadian Tire Information Resources. * Canadian Tire will provide relevant Information Security Policies to all personnel, including third parties and contractors, to ensure they understand their responsibilities in protecting Information Resources. * Personnel must review and acknowledge receipt of Information Security Policies before being granted access to Canadian Tire Information Resources. * The Training and awareness could be categorized into the following   + Training and awareness for Security - applicable to all employees   + Training and awareness for Business Continuity and Disaster Recovery - applicable to all employees   + Training and awareness after Incidence response - Applicable to SOC and CSIT team   Reference controls: SP 800-53 Rev. 5: AT-3, 4 |
| ***Compliance and Consequences*** | * Increased Security Risks: Untrained personnel might fall victim to phishing attacks or expose sensitive data unintentionally. * Potential Data Breaches: Lack of awareness about information security policies could lead to accidental or deliberate breaches, damaging Canadian Tire's reputation and incurring financial penalties. |

By enforcing these policies, Canadian Tire can mitigate these risks, protect its assets and reputation, ensure business continuity, and enhance its resilience against evolving threats in the digital landscape. Regular review and modification of these policies are essential to adapt to changing threats, technologies, regulations, and organizational needs, thereby maintaining a proactive stance in safeguarding its information assets and operations.

# INCIDENT RESPONSE PLAN

## Testing and Review Cycle

Anual testing of the Incident Response Plan using walkthroughs and practical simulations of potential incident scenarios is necessary to ensure the CSIRT is aware of its obligations unless real incidents occur that test the full functionality of the process.

1. The Incident Response Plan will be tested at least twice annually
2. the Incident Response Plan Testing will test Canadian Tire’s response to potential incident scenarios to identify process gaps and improvement areas.
3. The CSIRT will record observations made during the testing, such as steps that were poorly executed or misunderstood by participants and those aspects that need improvement.
4. The Incident Response Lead will ensure the Security Incident Response Plan is updated and distributed to CSIRT members

## Authority

Responsibility for the security of company and customer information typically resides with Chief Executive Officer, Chief Information Security Officer (CISO), CFO, and other C-suite executives.

During times when a high or critical cybersecurity incident is underway, the responsibility for managing the incident is typically entrusted to the Incident Response Team Head or Chief Information Security Officer (CISO)

The authority to identify and document the individuals/roles responsible for handling incidents within an organization typically lies with senior leadership, such as the CEO, executive management team, or the Chief Risk Officer (CRO) if the organization has one.

The process of identifying incident response roles and responsibilities often involves collaboration among various stakeholders, including executives, department heads, legal counsel, IT professionals, and other relevant personnel. It may also involve input from external advisors, such as legal experts or cybersecurity consultants, to ensure that the organization's incident response plan is comprehensive and effective.

## How to Recognize a Cyber Incident

This report is focused on IR policies and plans for Ransomware attacks. Ransomware attacks are a significant cybersecurity threat, and Canadian Tire (CTC) needs to be prepared to identify them quickly.

**System Access Issues:**

* *Widespread Lockouts:* A sudden increase in user reports of being unable to access critical applications or systems. This could indicate that ransomware has encrypted files, rendering them inaccessible.
* *Slow System Performance*: Unusual slowness or unresponsiveness across various systems could signal an ongoing attack or the deployment of ransomware in preparation for encryption.

**Data Anomalies:**

* *Unexplained File Modifications*: IT teams might detect unusual file extensions or modifications across servers or user workstations. This could be a sign of ongoing encryption by ransomware.
* *Data Exfiltration Attempts*: Network security tools might flag attempts to transfer large amounts of data outwards, potentially indicating stolen data exfiltration before encryption.

**Alerts and Notifications:**

* *Antivirus Alerts:* Antivirus software might trigger alerts for suspicious activity, potentially related to ransomware deployment or attempts to exploit vulnerabilities.
* *Security Information and Event Management (SIEM) Alerts*: SIEM systems could generate alerts for unusual network activity, unauthorized access attempts, or suspicious file modifications, which might be indicators of a ransomware attack.

**Communication and User Behavior:**

* *Phishing Attempts*: A surge in phishing emails targeting employees could be a precursor to a ransomware attack, attempting to gain initial access to the network.
* *Demand for Ransom Payments*: Employees or IT teams might receive messages demanding ransom payments to decrypt locked files, a clear sign of a ransomware attack.

**Canadian Tire's Specific Considerations:**

* *Point-of-Sale (POS) Disruptions*: Disruptions to POS systems at multiple stores could indicate a ransomware attack targeting critical business operations.
* *Supply Chain Impact:* If Canadian Tire's suppliers or partners experience ransomware attacks, it could disrupt product availability or logistics, impacting CTC's operations.

## Cyber Security Incident Response Team

An effectively functioning CSIRT requires an array of members with various skills and responsibilities. There is no one-size-fits-all approach, however. Organizations must staff and train employees to meet their specific security incident response needs. Several factors affect the organization of CSIRT roles, including the organization's risk profile and CSIRT structure. In general, CSIRT members include the following:

| **CSIRT Role** | **Role Definition** | **Escalation (1-3)\*** |
| --- | --- | --- |
| ***Executive*** | Accountable Executive for protecting cyber security within the organization. Responsible for reporting to board directors and other executives. Within the CSIRT, this role is responsible for all issues requiring executive decisions. | 1 |
| ***Incident Handler*** | The Incident Handler is the main triage role of the CSIRT. This role organizes the team and initiates the Incident Response Plan to investigate and respond to cyber security incidents. | 1 |
| ***Communications*** | The Communications Expert is responsible for both public relations and internal communications. They are the messenger to ensure that internal/external stakeholders, customers, and the public are informed in a timely and compliant fashion. | 2 |
| ***Network Administrator*** | The Network admin is responsible for setting up network architecture, maintaining the configuration, and monitoring the network activity. | 2 |
| ***System Administrator*** | The system admin is responsible for managing access control, and user permissions. Manage backup and recovery of server and endpoints. They assist with system recovery efforts, restoring affected systems and ensuring data integrity. | 3 |
| ***Security Analyst*** | These individuals are responsible for monitoring security logs, detecting threats, and conducting initial investigations. | 2 |
| ***Forensic Analyst*** | They specialize in collecting and analyzing evidence to determine the root cause of the incident and identify potential attackers. | 2 |
| ***Network Engineer*** | Network engineers play a crucial role in isolating infected systems, reconfiguring network settings, and ensuring network stability during the response. | 2 |
| ***Legal Advisor*** | The Legal advisor needs to make sure that the company's policies and procedures are meeting compliance with the laws and regulations. They also provide legal guidance on legal requirements, compliance issues, and potential legal actions related to the incident. | 3 |

\*Escalation level determines the order in which notification should occur:

1. Notify first
2. Required on all moderate or high severity incidents
3. Involve as needed

## CSIRT Responsibilities

The responsibilities described below are organized by role within **Canadian Tire Corporation**.

For contact information of the team, please refer to [Appendix: CSIRT Team Contact Information](#_ngdk95l4tkk7)

### Executives

The Executives are/is responsible for:

1. Meeting with the board of directors to best understand what is needed from a security point of view based on the organization’s business needs.
2. Making discussions with stakeholders for the allocation of budget for better functioning of the CSIRT team.
3. Executives oversee the organization's overall risk management strategy in response to a data breach. They work with the data breach response team to identify and assess risks, prioritize remediation efforts, and make informed decisions to manage risks effectively and minimize damage.
4. Regularly reporting any incidents and necessary cyber security actions to the board of directors and other executives.
5. Making decisions on the best way forward based on information provided by the CSIRT team.
6. Making sure that the roles within the CSIRT team are filled and the necessary tools/training are provided for employees to do their jobs.
7. Meeting with key roles within the CSIRT team to better understand what improvements can be made.

### Incident Handler

The Incident Handler is responsible for:

1. Making sure that the Incident Response Plan and associated response and escalation procedures are defined and documented. Ensure the handling of security incidents is timely and effective.
2. Make sure that the Incident Response Plan is up-to-date, reviewed, and tested, at least once each year.
3. Making sure that staff with Incident Response Plan responsibilities are properly trained, at least once each year.
4. Leading the investigation of a suspected breach or reported security incident and initiating the Incident Response Plan, as and when needed.
5. Reporting to and liaising with external parties, including the acquirer and card brands, legal representation, law enforcement, etc. as required.
6. Authorizing on-site investigations by appropriate law enforcement or payment card industry security/forensic personnel, as required. This includes authorizing access to/removal of evidence from the site.

### Communications Expert

The Communications Expert is responsible for:

1. Writing and sending internal and external communications about any incident that occurred.
2. Reporting any cyber incidents to the authorities if needed.
3. Interfacing with executives and other board members to provide information.
4. Interfacing with customers to provide regular updates about any incidents that may affect their experience.
5. Media engagement if needed during the incidence process.
6. Collecting customer responses for the impact of incidents, how they were handled, and any tips/suggestions.
7. Collecting lessons learned from members of the CSIRT team and updating management.

### CSIRT Team

Cyber Security Incident Response Team (CSIRT) members are responsible for:

1. Making sure that all staff understand how to identify and report a suspected or actual security incident.
2. Advising the Incident Handler of an incident when they receive a security incident report from staff. Coordinate with the incidence handler to choose the strategy.
3. Investigating each reported incident.
4. Taking action to limit the exposure of sensitive information or payment card data and to reduce the risks that may be associated with any incident.
5. Gathering, reviewing, and analyzing logs and related information from various central and local safeguards, security measures, and controls.
6. Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken in response to an incident.
7. Reporting each security incident and findings to the appropriate parties.
8. Helping law enforcement and card industry security personnel during the investigation processes. This includes any forensic investigations and prosecutions.
9. Resolving each incident to the satisfaction of all parties involved, including external parties.
10. Initiating follow-up actions to reduce the likelihood of recurrence, as appropriate.
11. Determining if policies, processes, technologies, security measures or controls need to be updated to avoid a similar incident in the future. They also need to consider whether additional safeguards are required in the environment where the incident occurred.

All staff members are responsible for:

1. Making sure they understand how to identify and report a suspected or actual security incident.
2. Reporting a suspected or actual security incident to the Incident Handler (preferable) or to another member of the Cyber Security Incident Response Team (CSIRT).
3. Reporting any security-related issues or concerns to line management, or to a member of the CSIRT.
4. Complying with the security policies and procedures of The Canadian Tire Corporation. This includes any updated or temporary measures introduced in response to a security incident (For example, for business continuity, incident recovery or to prevent recurrence of an incident).

## Incident Type and Severity Matrix

[Ransomware](https://www.crowdstrike.com/cybersecurity-101/ransomware/types-of-ransomware/) is a type of malware attack that encrypts a victim's data and prevents access until a ransom payment is made. Ransomware attackers often use social engineering techniques, such as phishing, to gain access to a victim's environment.

The CSIRT will determine the severity of the incident using a Ransomware Severity Matrix. This matrix considers several factors, including:

**Impact on Systems:**

* Whether a single system is affected or multiple systems are compromised.
* The criticality of the affected system(s) (e.g., production servers vs. individual workstations).

**Data Impacted:**

* Whether the attack impacts a single person's non-critical data or affects critical business data across the organization.
* The potential for data loss or exfiltration.

**Disruption Caused:**

* Whether a single person or multiple people are impacted by the attack.
* The scope of disruption, considering if it affects a single team/department, multiple teams/departments, or the entire organization.

**Recovery Time and Costs:**

* The estimated time to recover from the attack and restore functionality.
* The potential financial losses associated with downtime, data recovery, and ransom demands.

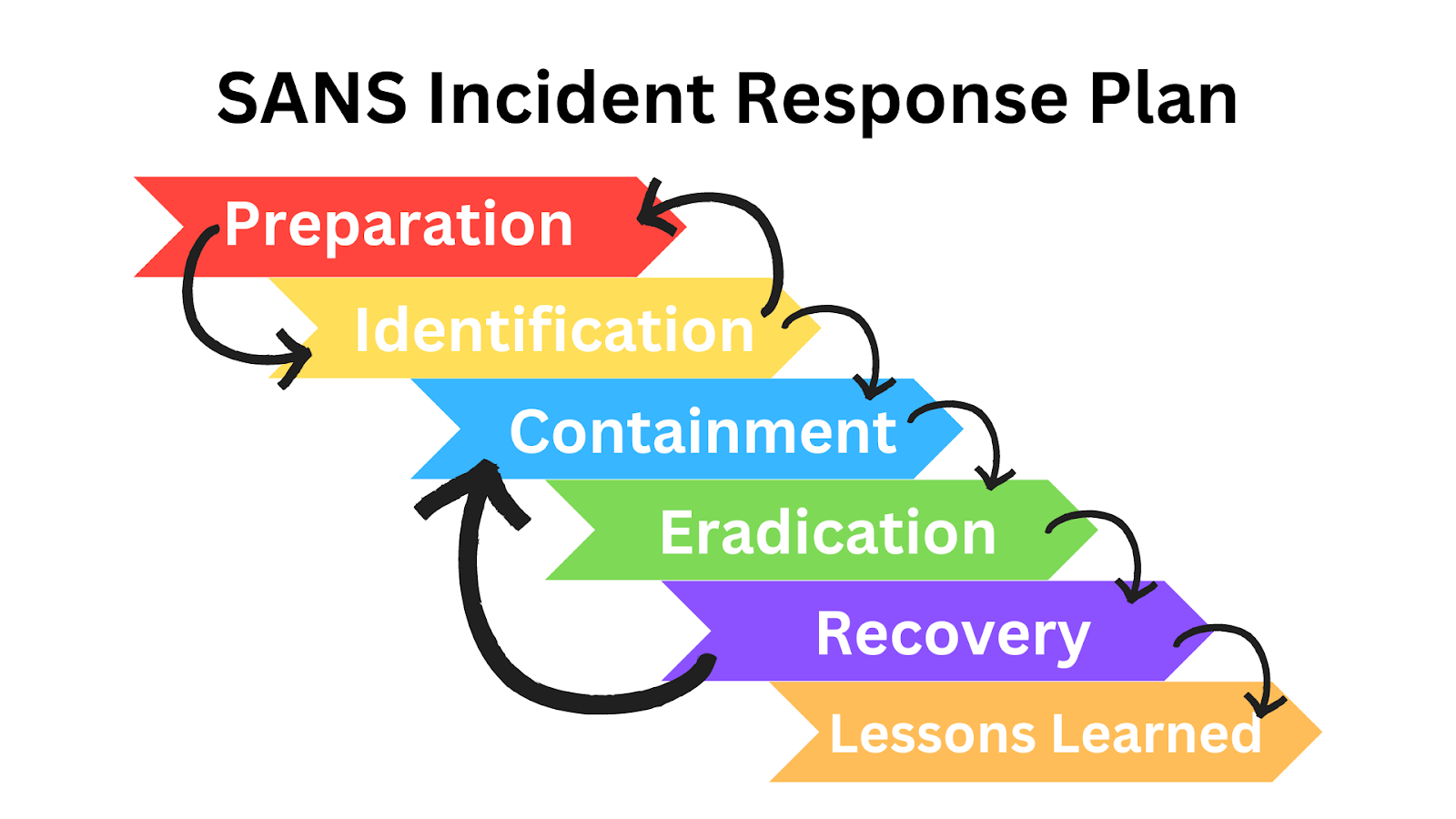
| **Factor** | **Low** | **Medium** | **High** | **Critical** |
| --- | --- | --- | --- | --- |
| **Data Impacted** | **Non-critical user data (e.g., documents)** | **Sensitive user data (e.g., financial records)** | **Critical business data (e.g., production systems)** | **All critical business data and backups compromised** |
| **System Downtime** | **< 1 hour** | **1-4 hours** | **4-8 hours** | **> 8 hours, significant disruption** |
| **Financial Impact** | **Minimal ransom demand** | **Moderate ransom demand** | **High ransom demand** | **High ransom demand, potential regulatory fines** |
| **Reputational Damage** | **Low impact on public image** | **Moderate impact on public image, potential customer concerns** | **Significant impact on public image, potential loss of customer trust** | **Severe impact on public image, potential loss of business** |
| **Recovery Time** | **< 1 day, minimal data loss** | **1-3 days, potential data loss** | **3-7 days, significant data loss** | **> 7 days, potentially irrecoverable data loss** |

## Incident Response Framework

Candian Tire recognizes that, despite reasonable and competent efforts to protect Information Resources, a breach or other loss of information is possible. The organization must make reasonable efforts and act competently to respond to a potential incident in a way that reduces the loss of information and potential harm to customers, partners, and the organization itself. ([SANS Image](https://wirexsystems.com/resource/sans-incident-response-framework/))

In Cyber security as per the NIST incident response lifecycle, Incident plans can be defined in 4 and according to SANS it is described in [6 phases](https://www.securitymetrics.com/blog/6-phases-incident-response-plan).

We will be discussing Incident response plans with distinct phases that will help SOC and IT professionals deal with cyber attacks. An incident response plan should be set up to address a suspected data breach in a series of phases. Within each phase, there are specific areas of need that should be considered.



The incident response phases are:

1. **Preparation:**

It is essential to establish a Cyber Security Incident Response Team (CSIRT), define appropriate lines of communication, articulate services necessary to support response activities, and procure the necessary tools.

1. **Identification:**

Identifying an event and conducting an assessment should be performed to confirm the existence of an incident. The assessment should include determining the scope, impact, and extent of the damage caused by the incident. In the event of possible legal action, digital evidence will be preserved, and forensic analysis may be conducted consistent with legislative and legal requirements.

1. **Containment:**

Containment of the incident is necessary to minimize and isolate the damage caused. Steps must be taken to ensure that the scope of the incident does not spread to include other systems and Information Resources. Root cause analysis is required prior to moving beyond the Containment phase and may require expertise from outside parties.

1. **Eradication**:

Eradication requires the removal or addressing of all components and symptoms of the incident. Further, validation must be performed to ensure the incident does not reoccur.

1. **Recovery:**

Recovery involves the steps required to restore data and systems to a healthy working state allowing business operations to be returned.

1. **Lessons Learned:**

The Lessons Learned phase includes post-incident analysis of the system(s) that were impacted by the incident and other potentially vulnerable systems. Lessons learned from the incident are communicated to executive management and action plans are developed to improve future incident management practices and reduce risk exposure.

# RANSOMWARE INCIDENT RESPONSE PLAYBOOK

This customized playbook outlines the steps for the Canadian Tire Cybersecurity Incident Response Team (CSIRT) to follow in the event of a ransomware attack. These steps should be completed sequentially, with some overlap expected during Containment, Eradication, and Recovery. ([referenced](https://frsecure.com/malware-incident-response-playbook/))

### Preparation

* **CSIRT Team:** Identify core CSIRT members focused solely on cybersecurity (refer to the [Cyber Security Incident Response Team](#_gtudrqm9iplt) section ).
* **Escalation Paths:** Establish clear escalation procedures based on incident severity.
* **Backups:** Ensure critical system backups are secure and regularly tested.

### Identification

* **Isolate Infected Systems:** Isolate infected systems immediately to prevent further spread. **Do not power them off.**
* **Forensic Preservation:** Preserve infected systems for forensic investigation (log review, memory analysis, etc.).
* **Malware Investigation:**
  + Determine if malware runs under a user account. If so, disable the account(s).
  + Analyze the malware characteristics to guide containment. Use a sandbox environment (disconnected from the network) whenever possible.
  + Identify Indicators of Compromise (IoCs) such as network connections, file modifications, and malware location.
  + Secure a copy of the malware in a password-protected archive with [SHA-256 hash](https://support.google.com/google-ads/answer/9004655?hl=en#:~:text=SHA%2D256%20stands%20for%20Secure,will%20create%20the%20same%20hash.) for further analysis using community resources ([VirusTotal](https://en.wikipedia.org/wiki/VirusTotal), etc.).
  + Utilize IoCs to identify additional infected systems and the initial point of entry (infection date, impacted user, potential infection vectors).
  + Research the ransomware variant to understand Tactics, Techniques, and Procedures (TTPs) associated with the attacker, including potential data exfiltration and extortion methods.

### Containment

* **Address Entry Point:** Use findings from the Identification phase to close potential entry points (e.g., firewall changes, email blocking, user education).
* **Isolate Additional Systems:** Isolate any additional infected devices identified using IoCs.
* **Endpoint Protection:** Update endpoint protection to block and alert on identified IoCs. Consider submitting the hash value to community sources for broader threat detection. (Consult legal/compliance for each incident).
* **Network Segmentation:** Implement temporary network rules and segmentation to contain the malware spread.
* **Disable Compromised Accounts:** Disable any additional compromised accounts discovered during the investigation.

### Eradication

* **Preserve Evidence:** Secure artifacts, systems, and relevant backups for potential future forensics.
  + For physical systems, preserve hard drives, solid-state drives, or forensically sound images.
  + For virtual machines, preserve a copy, full snapshot, or a backup of the system.
  + Secure any volatile data collected during Identification and Containment (logs, backups, malware samples, memory images).
* **System Restoration/Rebuilding:** Once evidence is secured, restore impacted systems from clean, pre-infection backups (if available). For non-restorable systems, rebuild from a known good image or bare metal.
* **Vulnerability Remediation:** Address any vulnerabilities and security gaps identified during the investigation.

### Recovery

* **Account Passwords:** Reset passwords for all impacted accounts or create replacements, and permanently disable compromised accounts.
* **Monitoring:** Maintain vigilance for continued malicious activity related to the incident. Configure alerts for quick detection and response.
* **Data Exfiltration & Extortion:** If data exfiltration and extortion are suspected, involve legal counsel to determine the next steps.

### Lessons Learned

* **Post-Incident Review:** Conduct a meeting to discuss the incident response, including:
  + Successes and challenges encountered during the investigation.
  + Identified vulnerabilities and security gaps.
  + Remediation plans for these vulnerabilities.
  + Potential preventative measures for future incidents.
* **Playbook Updates:** Evaluate the need for modifications to:
  + Network segmentation.
  + Firewall configurations.
  + Application security.
  + Patching procedures.
  + Employee, IT, and CSIRT training.
* **Incident Reporting:** Create and distribute an incident report for relevant parties:
  + A technical report for the CSIRT.
  + An executive summary of the management team.

# CONCLUSION

In conclusion, the adoption of suggested policies and a comprehensive ransomware incident response plan can serve as critical safeguards for Canadian Tire Corporation against the growing threat of ransomware attacks. By prioritizing cybersecurity measures, including robust data encryption, regular system backups, employee training on phishing awareness, and network segmentation, Canadian Tire can bolster its defenses against ransomware threats and minimize the likelihood of successful attacks.

By investing in proactive cybersecurity measures and establishing effective incident response protocols, Canadian Tire can enhance its resilience to ransomware threats, protect sensitive data assets, and uphold its commitment to maintaining the trust and confidence of customers, stakeholders, and regulatory authorities. In an increasingly digitized business environment, cybersecurity readiness is paramount, and Canadian Tire's proactive approach positions it strongly to navigate the evolving landscape of cyber threats and emerging challenges.

# 

# Appendix A: CSIRT Team Contact Information

Note: Due to Copyright and privacy we are not using the real name of Canadian Tire Corporation.

(!) Indicate assumptions

| **CSIRT Role** | **Name(!)** | **Title(!)** | **Phone(!)** | **Email(!)** |
| --- | --- | --- | --- | --- |
| Incident Handler\*\* (lead) | Misha F | Manager | 647-555-0001 | [mesha@cantire.com](mailto:mesha@cantire.com) |
| Incident Handler (Backup) | Minka D | General Manager | 647-555-0002 | [minka@cantire.com](mailto:minka@cantire.com) |
| Communications | Percy F. | President/Owner | 647-555-0001 | [percy@cantire.com](mailto:percy@cantire.com) |
| Network Admin | Dusty | Senior Network admin | 647-555-0014 | [dusty@cantire.com](mailto:dusty@cantire.com) |
| System Admin | Lucky S. | Senior System admin | 647-555-0002 | [lucky@cantire.com](mailto:lucky@cantire.com) |
| Security Analyst | John D. | Senior security analyst | 647-112-2055 | [john@cantire.com](mailto:john@cantire.com) |
| Forensic Analyst | Steven S. | Forensic Expert | 647-858-1578 | [steven@cantire.com](mailto:steven@cantire.com) |
| Network Engineer | Ned W. | Senior Network Engineer | 647-877-4332 | [ned@cantire.com](mailto:ned@cantire.com) |
| Legal Advisor | Yvonne C. | Legality Corp. | 647-555-0025 | [ylaurier@](mailto:ylaurier@legal.eg)cantire.com |
| Executive | Percy F. | President/Owner | 647-555-0001 | [percy@cantire.com](mailto:percy@cantire.com) |

### External Contacts

### 

| **Role (!)** | **Organization(!)** | **Name(!)** | **Title(!)** | **Phone(!)** | **Email(!)** |
| --- | --- | --- | --- | --- | --- |
| Network Security Vendor Support Lead | Cybersecurity Vendor Ltd. | Dante Williams | Support Lead | 647-555-0014 | [dwilliams@cv.eg](mailto:dwilliams@cv.eg) |
| Network Security Vendor | Cybersecurity Vendor Ltd. | General Helpdesk | Helpdesk | 1-888-555-0014 | [helpdesk@cv.eg](mailto:helpdesk@cv.eg) |
| Lawyer | Legality Corp. | Yvonne Laurier | Lawyer | 647-555-0025 | [ylaurier@legal.eg](mailto:ylaurier@legal.eg) |
| Parts Supplier | Supplier Co | Gina Asana | Account Manager | 647-555-0036 | [gina@supplier.eg](mailto:gina@supplier.eg) |
| Card Acquirer Service | POS Ltd. | Richard Kim | Account Manager | 647-555-0047 | [richard@pos.eg](mailto:richard@pos.eg) |
| Cyber Insurance Provider | Insurance Ltd.  Policy #123ABC | Mandy Singh | Account Manager | 647-555-0058 | [mandy@insurance.eg](mailto:mandy@insurance.eg) |
| Ransomware Decryption Service Provider | Ransomware Decryptor Inc. | Rachel D’Agostini | Account Manager | 647-555-0069 | [rachel@decryptor.eg](mailto:rachel@decryptor.eg) |
| Law Enforcement (local) | Toronto Police Local Precinct | Toronto Police | N/A | 647-911-0911 | [report@police.eg](mailto:report@police.eg) |

# 

# 

# 

# 

# 

# Appendix B: Stakeholder Communications

| **Stakeholder Groups** | **Engagement Triggers** |
| --- | --- |
| **Customers** | * If there is any breach that could impact them * Product recalls or safety hazards. * Changes to product offerings or store locations. * Loyalty program updates or promotions. |
| **Employees** | * During any incident ( SOC, CSIRT, and other Security teams) * Changes in company policy or benefits. * Training and Awareness discussion * Workplace safety incidents. |
| **Dealers** | * New marketing campaigns or product launches. * Changes to store operating procedures. * Profit-sharing programs or performance updates. |
| **Investors** | * Quarterly financial results and earnings calls. * Changes in company leadership or strategy. * Acquisitions or divestitures. * Any Cyber incident that could impact the funding(They should be informed after all cyber incidents in general) |
| **Suppliers** | * New product development opportunities. * Changes in sourcing or procurement practices. * Sustainability initiatives impacting the supply chain. |
| **Community** | * Sponsorship announcements or charitable giving activities. * Environmental impact initiatives. * Store openings or closures in specific communities. |
| **Government** | * Regulatory changes that impact Canadian Tire's operations. * Product safety compliance issues. * Public policy initiatives relevant to the retail industry. |

# 

# REFERENCES

1. *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#:~:text=for%20an%20organization.-,Why%20Do%20We%20Need%20an%20Incident%20Response%20Policy%3F,incident%20response%20for%20the%20organization>.
2. *Canadian Tire Corporation, Limited - about us*. (n.d.). <https://corp.canadiantire.ca/English/about-us/default.aspx>
3. Gowsika. (2024, April 9). *Incident Management Policy (What does it include?)*. Sprinto. <https://sprinto.com/blog/incident-management-policy/#:~:text=The%20incident%20policy%20defines%20the,seamless%20management%20and%20timely%20resolution>)
4. *ISO 22301 - Business continuity*. (2019). ISO. <https://www.iso.org/publication/PUB100442.html>
5. Montag, G. (2023, February 7). *SANS Incident Response Framework*. WireX. <https://wirexsystems.com/resource/sans-incident-response-framework/>
6. NewRocket, LLC. (n.d.). *Planning for the unexpected with business continuity management | NewRocket*. <https://www.newrocket.com/articles/planning-for-the-unexpected-with-business-continuity-management>
7. *SHA-256 Algorithm: Definition - Google Ads Help*. (n.d.). <https://support.google.com/google-ads/answer/9004655?hl=en#:~:text=SHA%2D256%20stands%20for%20Secure,will%20create%20the%20same%20hash>.
8. *What is penetration testing? | What is pen testing? | Cloudflare*. (n.d.). <https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/>
9. Wikipedia contributors. (2024, April 29). *VirusTotal*. Wikipedia. <https://en.wikipedia.org/wiki/VirusTotal>
10. 6 phases in the Incident Response plan. (n.d.). Securitymetrics. https://www.securitymetrics.com/blog/6-phases-incident-response-plan