Security Incident Response Plan

By: Danielle Daza

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document aims to provide a detailed summary of roles and responsibilities of the most relevant parties in regards to incident response as well as delineate an in-depth overview of incident response.

The roles and responsibilities covered in this report go over not only the technical experts that are responsible for actively investigating and resolving an incident but also include the duties of management, legal and compliance teams, HR, communications team, and employees in general in regards to handling the ripple-effects of an incident (i.e. making high-level decisions, ensuring actions are legal and compliant with regulations, updating employees of potential security breaches, etc.). As the Incident Response Team is the central team in handling incidents as they occur, more specific duties and responsibilities have been defined as well as team member-specified responsibilities have been summarized in a comprehensive table.

The incident response steps have been summarized following the US government-standard NIST Incident Handling Response documentation. These incident response steps have been used as a template for the logical development of the playbook also included in this report. The playbook provided is for phishing attacks with a summary flowchart to succinctly convey the core elements in a visual format. Triggers for escalation and conditions warranting stakeholder notifications have also been compiled into summarizing tables for reference. The entirety of this document is classified as Red under Traffic Light Protocol (TLP) as it contains personal contact information and additional sensitive information not to be shared with irrelevant parties.

ROLES AND RESPONSIBILITIES

This Security Incident Response Plan must be followed by all personnel, including all employees, temporary staff, consultants, contractors, suppliers and third parties operating on behalf of the organization. All personnel are referred to as 'staff' within this plan.

Below are details about the roles and responsibilities of each member of the organization to prevent and respond to a workplace incident. It is not an exhaustive list of duties but designed to give each employee a general understanding of their role and the roles of other employees in incident response and prevention.

TEAM ROLES AND RESPONSIBILITIES

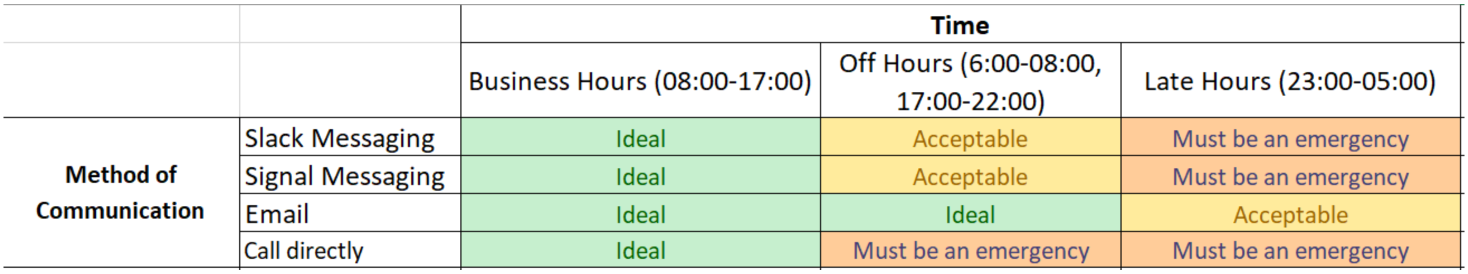
Below is a table that outlines the over-arching responsibilities across the relevant departments in the incident response process.

Role	Responsibility	Contact Details
Information Security		
CISO	• Strategic lead. Develops technical, operational, and financial risk ranking criteria used to prioritize incident response plan. • Authorizes when and how incident details are reported. • Main point of contact for executive team and Board of Directors.	Clinton McFadden cmcfadden@canadiantire.com Office: 416-123-4567 Cell: 647-123-4567
Information Security		
SOC Analysts	• Handle real-time monitoring and threat detection • Focuses on initial detection and triage of alerts. • Escalates incidents to the Incident Response Team for deeper investigation and remediation.	Manager – Neil Dover ndover@canadiantire.com Dept: 416-223-4567 Cell: 647-223-4567

Incident Response Team Lead and Team Members	• Central team that authorizes and coordinates incident response across multiple teams and functions through all stages of an incident. • Maintains incident response plan, documentation, and catalog of incidents. • Responsible for identifying, confirming, and evaluating extent of incidents. • Conducts random security checks to ensure readiness to respond to a cyberattack.	Lead – Sally Keyton skeyton@canadiantire.com Dept: 416-323-4567 Cell: 647-323-4567
IT/Network Admin Team Members	• Implements and ensures the security measures and system configurations are performing accordingly. • Follow incident response procedures to preserve evidence to report to the Incident Response Team and assist in some capacity in investigating the incident.	Manager – Alan Beck abeck@canadiantire.com Dept: 416-423-4567 Cell: 647-423-4567
Compliance		
Legal Counsel	• Confirms requirements for informing employees, customers, and the public about cyber breaches. • Responsible for checking in with local law enforcement. • Ensures IT team has legal authority for privilege account monitoring.	Lead – Will Vera wvera@canadiantire.com Dept: 416-523-4567 Cell: 647-523-4567
Audit & Compliance	• Communicates with regulatory bodies, following mandated reporting requirements.	Lead – Ben Roache broache@canadiantire.com Dept: 416-623-4567 Cell: 647-623-4567
Human Resources	• Coordinates internal employee communications regarding breaches of personal information and responds to questions from employees.	Lead – Samantha Stevens sstevens@canadiantire.com Dept: 416-723-4567 Cell: 647-723-4567
Regulatory Contact	• Receives information about a breach according to timeline and format mandated by regulatory requirements.	Hugh Blevins hblevins@canadiantire.com 647-823-4567
Communications		

Marketing & Public Relations Lead	- Communicates externally with customers, partners, and the media. - Coordinates all communications and request for interviews with internal subject matter experts and security team. - Maintains draft crisis communications plans and statements which can be customized and distributed quickly in case of a breach.	Beatrice Fleck bfleck@canadiantire.com 647-923-4567
Web & Social Media Lead	- Posts information on the company website, email, and social media channels regarding the breach, including our response and recommendations for users. - Sets up monitoring across social media channels to ensure we receive feedback or questions sent by customers through social media.	Paige Turner pturner@canadiantire.com 647-113-4567
Technical Support Lead (Internal)	- Provides security bulletins and technical guidance to employees in case of a breach, including required software updates, password changes, or other system changes.	Tina O'Shea toshea@canadiantire.com 647-133-4567
Technical Support Lead (External)	- Provides security bulletins and technical guidance to external users in case of a breach.	Irene Beach ibeach@canadiantire.com 647-143-4567

Below is a table outlining acceptable methods of communication in relation to the time of day another employee/manager's attention is required in the event of an incident taking place. The purpose of the table is to ensure that there is no confusion or apprehension about when is the most appropriate time to notify an individual or what method is acceptable at any particular time.



		Time		
		Business Hours (08:00-17:00)	Off Hours (6:00-08:00, 17:00-22:00)	Late Hours (23:00-05:00)
Method of Communication	Slack Messaging	Ideal	Acceptable	Must be an emergency
	Signal Messaging	Ideal	Acceptable	Must be an emergency
	Email	Ideal	Ideal	Acceptable
	Call directly	Ideal	Must be an emergency	Must be an emergency

INCIDENT RESPONSE TEAM RESPONSIBILITIES

Below is a breakdown of the expected responsibilities of the central Incident Response Team and general employees of Canadian Tire.

	Responsibilities
Incident Response Lead	• Making sure that the Security Incident Response Plan and associated response and escalation procedures are defined and documented. This is to ensure that the handling of security incidents is timely and effective. • Making sure that the Security Incident Response Plan is current, reviewed and tested at least once a year. • Making sure that staff with Security Incident Response Plan responsibilities are properly trained at least once a year. • Leading the investigation of a suspected breach or reported security incident and initiating the Security Incident Response Plan when needed. • Reporting to and liaising with external parties, including pertinent business partners, legal representation, law enforcement, etc., as is required. • Authorizing on-site investigations by appropriate law enforcement or third-party security/forensic personnel, as required during any security incident investigation. This includes authorizing access to/removal of evidence from site.
Incident Response Team members	• Making sure that all staff understand how to identify and report a suspected or actual security incident. • Advising the Incident Response Lead of an incident when they receive a security incident report from staff. • Investigating and documenting each reported incident. • Taking action to limit the exposure of sensitive data and to reduce the risks that may be associated with any incident. • Gathering, reviewing, and analyzing logs and related information from various central and local safeguards, security measures and controls. • Documenting and maintaining accurate and detailed records of the incident and all activities that were undertaken in response to an incident. • Assisting law enforcement during the investigation processes. This includes any forensic investigations and prosecutions. • Initiating follow-up actions to reduce likelihood of recurrence, as appropriate. • 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	• Making sure they understand how to identify and report a suspected or actual security incident. • Reporting a suspected or actual security incident to the Incident Response Lead (preferable) or to another member of the Security Incident Response Team (SIRT). • Reporting any security related issues or concerns to line management, or to a member of the SIRT. • Complying with the security policies and procedures of Canadian Tire.

Below is a summary table that defines the roles and responsibilities of the Incident Response Team members in the event of an incident. This table aims to aid in clarify the capacities in which all the team members would be involved in the entire process of incident handling. Furthermore, responsibility definitions have been provided to detail the capacity of each term used in the table.

Responsibility definitions:

i. **Owner**: is held accountable for the progression, decision-making and ultimate result of the action.

ii. **Implements**: under the management of the Owner, assists in the implementation of the action.

iii. **Updates**: provides updates on the incident to the Owner so they have all relevant information to proceed and make appropriate judgements on the situation

iv. **Advises**: provides guidance and advice to the Owner that would be beneficial in the decision-making process.

v. **None**: does not play any role in this action.

Action	Role				
	Incident Response Lead	**IT Contact**	**Legal Representative**	**Communications Officer**	**Management**
Initial Assessment	Owner	Advises	None	None	None
Initial Response	Owner	Implements	Updates	Updates	Updates
Collects Forensic Evidence	Implements	Advises	Owner	None	None
Implements Temporary Fix	Owner	Implements	Updates	Updates	Advises
Sends Communication	Advises	Advises	Advises	Implements	Owner
Check with Local Law Enforcement	Updates	Updates	Implements	Updates	Owner
Implements Permanent Fix	Owner	Implements	Updates	Updates	Updates
Determines Financial Impact on Business	Updates	Updates	Advises	Updates	Owner
Documentation	Owner	Advises	Advises	None	None

References: (CichonskiPaul, MilarTom, GranceTim, ScarfoneKaren, 2012)

INCIDENT RESPONSE PROCESS OVERVIEW

Below is a 7-step process outlining the basic steps in necessary in incident response as stipulated by the US government-standard NIST Incident Handling Response document. This process has been utilized as a template for steps to follow in handling specific incidents or breaches.

Incident Response Process Step	Objectives and Outcomes
Preparation	1. Review and codify an organizational security policy. 2. Perform a risk assessment, identify sensitive assets, define which are critical security incidents the team should focus on, and build a Computer Security Incident Response Team (CSIRT).
Detection	3. Monitor IT systems and detect deviations from normal operations and see if they represent actual security incidents.

Incident Analysis	4. Analysis to understand the nature of the incident and potential malware or threat actors involved. 5. Identify o Systems affected (i.e. Servers, Desktop, Laptop) and/or at risk. o User credentials compromised or at risk. o Any malicious code and on what systems. o Any IT services impacted. o Business implications due to the attack. o Tools used to detect the attack.
Containment	6. Determine the necessary containment strategy to prevent further damage. E.g. o Isolate the devices involved, removing it from the shared network system o Relegate any responsibilities/processing from affected systems onto a backup system
Eradication	7. Eliminate the threat involved. E.g. o Adjust Firewall rules. o Eradicate malware. o Patching software. o Changing compromised credentials.
Recovery	8. Recover affected systems and data. E.g. o Restoring backups. o Reinstalling software. 9. Resetting credentials, implementing Multi-Factor Authentication (MFA).
Post-Incident Analysis and Reporting	10. Identify what was learned from the incident and what can be done to prevent similar incidents in the future. 11. Provide a detailed overview of the incident, its impact on operations, the response actions taken, and recommendations for future prevention. 12. Update policies and procedures if needed.

References: (NelsonAlex, RehkiSanjay, SouppayaMurugiah, ScarfoneKaren, 2024) (CichonskiPaul, MilarTom, GranceTim, ScarfoneKaren, 2012)

PHISHING ATTACK PLAYBOOK

Below is a phishing incident response playbook in a table format with specified actions and responsible members of the organization included for each Incident Response Process Step. Following this table version will be a flowchart that visually conveys the steps and essential actions of the playbook.

IRP Step	Responsible Members	Action
Prepare	**CISO** – ensures the organization has a comprehensive phishing response plan and oversees preparation activities **Network Administrators** – set up and maintain anti-phishing tools, email filtering, and security protocols to block malicious emails **HR**– implements the phishing awareness training for all employees **Legal/compliance teams** – ensure the phishing incident response activities comply with regulatory requirements **Incident Response team** – develops playbook for phishing incidents, detailing response steps, stakeholder communication procedures and post-incident analysis.	1. Phishing awareness training on recognizing a common tactics used (e.g. urgent messages, suspicious links, fake sender addresses). 2. Implement anti-phishing technologies like email filtering and endpoint security. 3. Develop incident response playbook for phishing incidents, including detailed response steps, stakeholder communication procedures, and post-incident actions. 4. Establish clear communication channels (e.g. ticketing system) where employees can easily report phishing emails.
Detection	**General employees (end users)** – notify the IT or security teams if they suspect a phishing email or link **SOC Analysts** – investigates suspicious emails or user behavior in the network	5. Using email security tools to detect known malicious email signatures, suspicious attachments and links. 6. Use Security Information and Event Management (SIEM) tools to correlate logs form email servers and firewalls to detect suspicious activity associated with phishing attempts. 7. Initial triage ○ Assess if the phishing email was successful in luring any employee to click on any sent links, or entered credentials. ○ Confirm if it is a genuine positive or a false positive.
Incident Analysis	**Incident Response team** – coordinates with the affected teams, helping in classifying the incident and escalating the incident if necessary **IT/Network admin teams** – collects additional information from the affected users and assists in identifying whether their systems were compromised.	8. Forensic analysis - collect and preserve evidence for post-incident analysis (e.g. logs, screenshots, emails). ○ If malware was downloaded, analyze the behaviour of the malware to understand the its capabilities (e.g. ransomware, credential harvesting). 9. Determine impact ○ Identify which employees or systems are affected by the phishing attempt. ○ Assess if any sensitive or vital information was accessed.

		○ Confirm if the phishing attack has led to further lateral movement within the network.
Containment	**Incident Response team** – makes decisions on containment measures and ensures quick implementation or appropriate actions **IT/Network admin teams** – block malicious IPs, URLs, and email addresses used in the phishing attempt as well as block compromised accounts and reset passwords **HR and Communications teams** – internal communication to employees to ensure they stop interacting with phishing emails and make steps towards changing any compromised credentials	10. Isolate the affected system from the network immediately. 11. Suspend login credentials for compromised accounts. 12. Quarantine the malicious emails. ○ Remove the phishing email from all users' inboxes. ○ Block the malicious sender email address and domain from the email system. 13. Block all malicious URLs found in the alerts (and IP addresses) with firewall configurations. 14. Monitor for any lateral movement that may need to be addressed as well in the eradication step.
Eradication	**Incident Response team** - coordinates efforts to ensure all phishing related files, URLs, and malicious artifacts are removed from systems **IT/Network admin teams** – conducts deeper scans to remove and verify the removal of any traces of malicious objects within the compromised systems	15. Run anti-malware scans on affected systems to ensure any malicious files are removed. 16. Ensure that any malicious content that may be present (e.g. files, scripts) are fully removed from the email system. 17. Apply necessary patches and strengthen security controls.
Recovery	**Incident Response team** – overseas the recovery process, ensures that necessary post-incident actions are taken, confirms that the affected systems are safe to return to normal **Network administrators** – restores affected systems, ensures necessary patches have been applied, resets passwords for compromised accounts **HR and Communication teams** – notified employees about recovery steps and provides guidance on monitoring their personal and work accounts for signs for future attacks	18. Restore affected systems once they have been cleaned and secure for normal operations. 19. If user accounts were compromised, reset and ensure the use of multi-factor authentication. 20. Monitor the email traffic, user activity and network traffic for anomalies.
Post-Incident Analysis and Reporting	**CISO** – reviews the incident response performance and identifies strategic changes to security posture, policies, or tools	21. Document details of the incident, specific actions taken, and eventual solutions in an incident report. 22. Analyze the root cause and review any vulnerabilities or weaknesses in the system that

	Incident Response team – leads the post-incident review, gathering data from involved teams, and documents the incident response process and areas of improvement **IT/Network admin teams** – suggest improvements that could be implemented in the network or infrastructure based on the vulnerabilities exposed during the incident **Legal/Compliance teams** – ensure that the organization complies with any regulatory obligations regarding post-incident reporting and breach notification **HR** – reviews training effectiveness and consult with the incident response team about updating the training programs as needed **Communications team** – prepares any necessary public statements or internal communications based on the outcome of the post-incident analysis	allowed the phishing attack to succeed (e.g. lack of email filtering, lack of employee awareness). 23. Update security protocols, strengthen phishing detection and review incident response procedures for any oversight. 24. If sensitive data was exposed, notify regulatory authorities about the incident in accordance with data breach notification laws. 25. Update phishing awareness training with real examples from the incident to educate employees about evolving phishing tactics. ○ Consider follow-up with phishing simulations to assess the effectiveness of updated training.

References: (AndersonGrady, 2024) (iCybersecurity, 2021) (Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook, 2012) (CloudGoogle, 2023) (Incident Response Team Depth Chart: Roles & responsibilities, 2024) (Top 8 Incident Response Plan Templates and Why You Should Automate Your Incident Response, 2024) (Security Orchestration and Automation Playbook, 2019)

FLOWCHART

Below is a flowchart that succinctly conveys the core elements of the phishing incident response process.

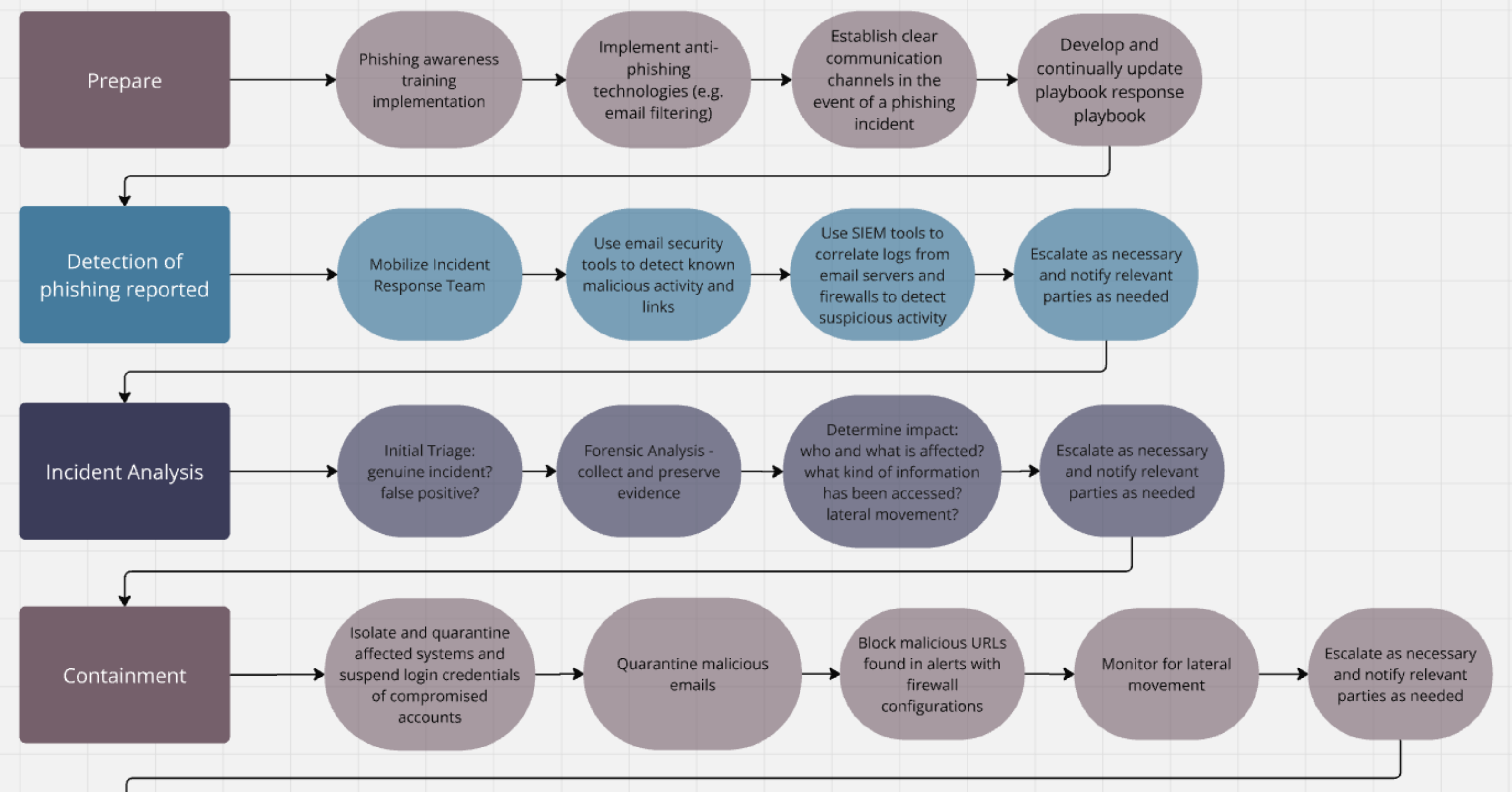

Prepare
Phishing awareness training implementation
Implement anti-phishing technologies (e.g. email filtering)
Establish clear communication channels in the event of a phishing incident
Develop and continually update playbook response playbook
Detection of phishing reported
Mobilize Incident Response Team
Use email security tools to detect known malicious activity and links
Use SIEM tools to correlate logs from email servers and firewalls to detect suspicious activity
Escalate as necessary and notify relevant parties as needed
Incident Analysis
Initial Triage: genuine incident? false positive?
Forensic Analysis - collect and preserve evidence
Determine impact: who and what is affected? what kind of information has been accessed? lateral movement?
Escalate as necessary and notify relevant parties as needed
Containment
Isolate and quarantine affected systems and suspend login credentials of compromised accounts
Quarantine malicious emails
Block malicious URLs found in alerts with firewall configurations
Monitor for lateral movement
Escalate as necessary and notify relevant parties as needed

Figure 1.1 – Phishing Incident Response Playbook 1/2

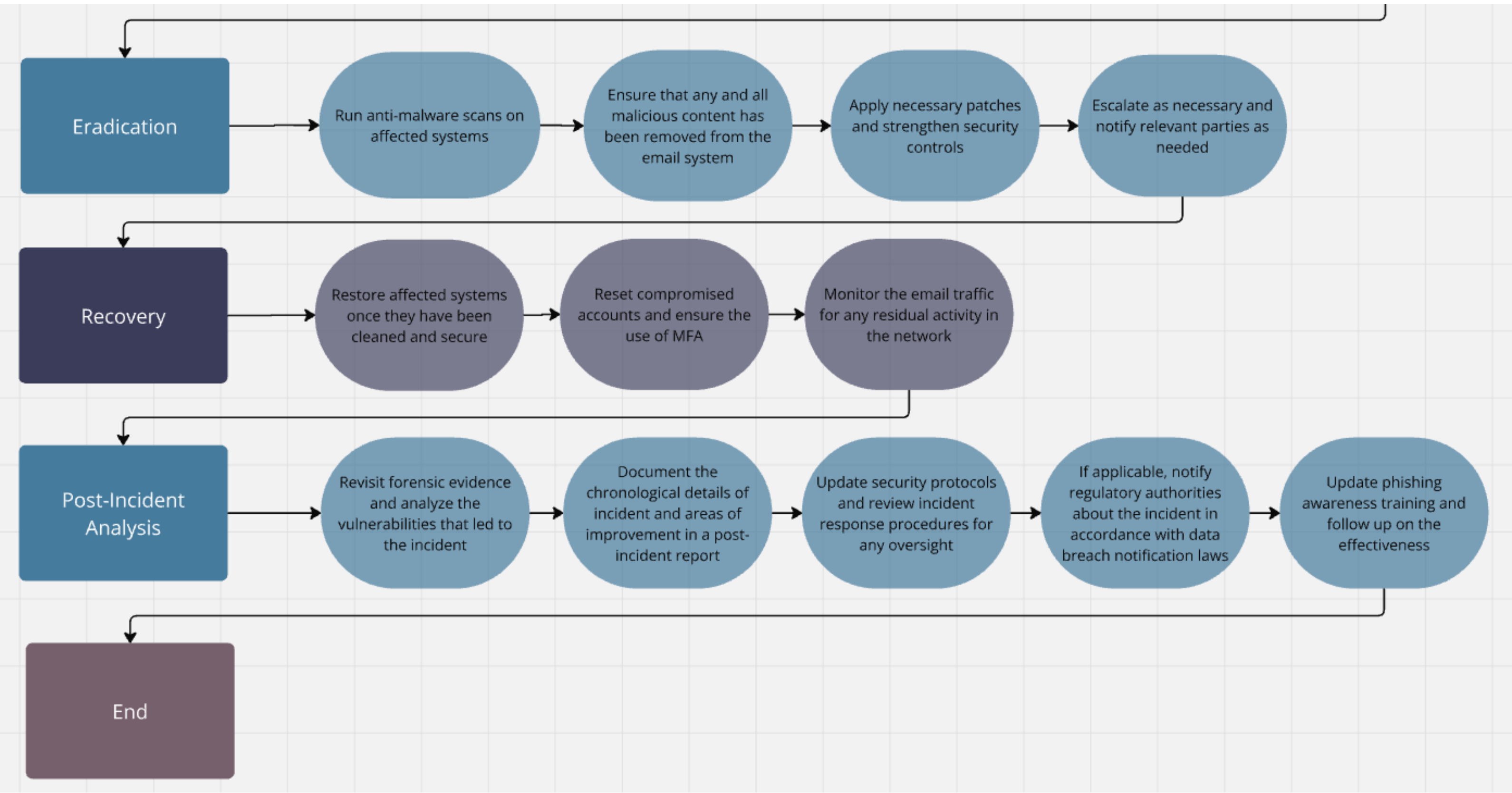

Eradication
Run anti-malware scans on affected systems
Ensure that any and all malicious content has been removed from the email system
Apply necessary patches and strengthen security controls
Escalate as necessary and notify relevant parties as needed
Recovery
Restore affected systems once they have been cleaned and secure
Reset compromised accounts and ensure the use of MFA
Monitor the email traffic for any residual activity in the network
Post-Incident Analysis
Revisit forensic evidence and analyze the vulnerabilities that led to the incident
Document the chronological details of incident and areas of improvement in a post-incident report
Update security protocols and review incident response procedures for any oversight
If applicable, notify regulatory authorities about the incident in accordance with data breach notification laws
Update phishing awareness training and follow up on the effectiveness
End

Figure 1.2 – Phishing Incident Response Playbook 2/2

References: (NCC Group, 2024) (CloudGoogle, 2023)

KEY TRIGGERS THAT WARRANT ESCALATION

Below is a summary table outlining the most notable triggers that would warrant the need for escalation. The following table will break down where that trigger is most likely to be discovered, the trigger itself, the level of escalation needed for the trigger, and the rationale behind why certain triggers may require certain teams' attention.

Step Trigger is Discovered	Trigger	Action	Rationale
Detection	Successful phishing attack that involves compromised credentials or malware infection.	Escalated to Incident Response Team for next IR steps	• If an attacker is able to gain access to user credentials, they can compromise sensitive data and escalate the access within the network.
Detection	High-profile involvement (spear-phishing).	Escalate to Tier 2 Analysts for further investigation	• There is a potential for significant financial or reputational damage given the nature of a spear-phishing attempt.
Incident Analysis	Data breach involving customer data	Escalate Incident Response Team and involve regulatory authorities	• These situations have the potential for compliance violations and legal consequences. • Company reputation could be severely damaged if the public disclosure is not appropriately handled by the communications team.
Containment	Social engineering or impersonation to escalate privileges.	Escalate to Incident Response Team and involve IT/Network admin teams and notify management.	• With impersonation being observed, financial fraud (e.g. wire transfer) is also a possibility. • The attacker may be using advanced tactics to gain access to systems or data (e.g. evading email filters).

Eradication	Evidence of lateral movement or further network compromise.	Escalate to crisis management and may need to involve external stakeholders.	• An increased attack surface could lead to widespread infection such as lateral movement across the network. • Observed lateral movement from the simple phishing attack implies there may be a more sophisticated targeted campaign. • If the attack is not contained and the attack continues to escalate, it could result in critically substantial consequences both financially and reputational.

Additionally, when determining the severity of particular attacks, it is important to also take into account the following escalation factors as well before actively escalating the incident.

Key Escalation Factors to Consider:

i. **Impact** – how severe is the attack in terms of data, systems, financial consequence?

ii. Scope – how many employees, systems, or departments are affected? Are customers affected?

iii. **Type of attack** – is it a targeted spear-phishing attack? Is it a widespread mass phishing campaign?

iv. **Data compromise** – has the sensitive data been exposed or stolen? Or corrupted?

v. **Compliance** – are there regulatory or legal reporting requirements?

CONDITIONS THAT WARRANT STAKEHOLDER NOTIFICATION

Below is a summary table outlining particular conditions that would warrant notifying internal or external stakeholders about an incident. It is expected that any and all **relevant** information to the parties in need of notification is provided. Depending on the nature of the phishing attack and the data that may be involved, an inevitable overlap in notifying both internal and external stakeholders may occur. It is advised to refer to the "**Key Escalation Factors to Consider**" heading earlier in this report when considering the additional stakeholders to notify.

Condition	Internal/External Stakeholders	Rationale
Sensitive data is compromised, financial fraud suspected, or attack may result in regulatory or legal issues.	Internal stakeholders - legal and compliance teams	This team needs to assess the situation from a legal and compliance perspective, including data protection laws.
The phishing attack involves high-profile individuals (e.g. executives).	Internal stakeholders - Executive Leadership	Executive leadership needs to be informed to make critical decisions, especially if the attack could impact Canadian Tire's reputation, finances, or ongoing operations.
The phishing attack's attack surface is wide enough to likely be publicly disclosed or could damage the Canadian Tire's reputation.	Internal stakeholders – public relations (PR) and communications team	The PR and communications teams can help manage public perception, develop appropriate messaging for external communications (i.e. media, customers, shareholders) and ensure consistent updates are being delivered to the relevant parties.
The phishing attack results in the exposure of personal, sensitive, or regulated data (e.g. PII, financial records).	External stakeholders – regulatory agencies	Regulations such as GDPR, HIPAA and CCPA require prompt notification of breaches involving personal data, often within a specified timeframe.
The phishing attack compromises customer data, business-critical partner relationship, or vendor systems.	External stakeholders – customers, partners, vendors	In order to best comply with privacy regulations, it is imperative to notify the affected parties, especially if their data or systems were impacted.

REFERENCES

Anderson, G. (2024, January 18). *The Role of Network Administrators in Ensuring Data Security*. Retrieved from MoldStud: https://moldstud.com/articles/p-the-role-of-network-administrators-in-ensuring-data-security

Canadian Tire. (2024). Retrieved from Policies: https://www.canadiantire.ca/en/customer-service/policies.html

Canadian Tire. (2024). Retrieved from Our Leadership Team: https://corp.canadiantire.ca/English/about-us/executive-management/default.aspx

Cichonski, P., Milar, T., Grance, T., & Scarfone, K. (2012). *Computer Security Incident Handling Guide.*

Cloud, G. (2023). *Top Security Playbooks.* Whitepaper.

i, C. a. (2021). *Cybersecurity Incident & Vulnerability Response Playbooks.*

Incident Response Team Depth Chart: Roles & responsibilities. (2024, August 23). Retrieved from Wiz: https://www.wiz.io/academy/incident-response-team

Meeting Data Compliance with a Wave of New Privacy Regulations: GDPR, CCPA, PIPEDA, POPI, LGPD, HIPAA, PCI-DSS, and More. (2019, September 17). Retrieved from NetApp: https://bluexp.netapp.com/blog/data-compliance-regulations-hipaa-gdpr-and-pci-dss

NCC Group. (2024). *Cyber Incident Response Phishing Playbook v2.4.*

Nelson, A., Rehki, S., Souppaya, M., & Scarfone, K. (2024). *Incident Response Recommendations and Considerations for Cybersecurity Risk Management.* U.S Department of Commrce.

O'Shea, S. (2017, February 8). *Canadian Tire admits 5 days after breach customer info may have been 'accessed'.* Retrieved from Global News: https://globalnews.ca/news/3236903/exclusive-canadian-tire-website-breached-consumer-accounts-in-question/

Policy Statement Examples. (2024). Retrieved from Wayne State University: https://policies.wayne.edu/policy-statement-examples

(2019). *Security Orchestration and Automation Playbook.* Rapid7.

Special Publication 800-12: An Introduction to Computer Security: The NIST Handbook. (2012, January 31). Retrieved from NIST: https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter3.html

Top 8 Incident Response Plan Templates and Why You Should Automate Your Incident Response. (2024, November 20). Retrieved from Cynet: https://www.cynet.com/incident-response/incident-response-plan-template/

What is Email Authentification? (2022). Retrieved from Validity: https://www.validity.com/email-authentication/