# IR Plan, Playbook and Policy

## BC Ferries

---

Prepared by: Prinson D'silva
Date: January 25th, 2025

# Table of Contents

## Executive Summary

This project focuses on developing an Incident Response Plan for the organization, BC Ferries in the event of a Ransomware attack. It integrates a detailed Ransomware Incident Response Playbook with high-level organizational security policies to ensure swift, structured, and compliant responses to the related security incident. The plan minimizes operational disruptions, protects sensitive data, and fosters regulatory compliance.
According to IBM, a Ransomware is a type of malware that holds a victim's sensitive data or device hostage, threatening to keep it locked or worse, unless the victim pays a ransom to the attacker. [Matthew Kosinski, January 2025]

The Incident Response Plan is based on four key steps as highlighted in the NIST Special Publications 800-61v2:

- **Preparation:** This step ensures the organization is ready to respond to the incident by developing **incident response policies**, defining roles and responsibilities of the team overlooking incidents while focusing on preventing incidents by ensuring that systems, networks, and applications are sufficiently secure.
- **Detection and Analysis**: In this step, the security events and incidents are detected and analyzed as various tools and technologies for monitoring and detecting potential security incidents are put into practice. After an incident is detected, it undergoes analysis to understand its nature, impact, and scope while determining the severity and priority of the incident.
- **Containment, Eradication and Recovery**: After confirming the incident, it is contained to prevent further damage by developing a tailored strategy which is highlighted in our **incident response playbook**, followed by eradication which involves removing or the cause of the incident. Finally, the recovery phase involves restoring affected systems, verifying their integrity, and ensuring normal operations are resumed.
- **Post-Incident Activity**: This includes conducting a thorough review and analysis of the incident response process to identify any areas for improvement. Lessons learned from the incident are documented, and recommendations are made to enhance security controls, update incident response plans, and address any gaps or vulnerabilities identified during the incident.
  [Paul Cichonski et al., 2012]

After implementing this incident response plan, the following requirements have been fulfilled:

- Each policy directly links to the playbook's actionable steps, aligning strategic objectives with operational execution.
- The incident response plan adheres to PIPEDA, PCI DSS, and other regulatory requirements, with escalation and reporting templates for both internal and external stakeholders.
- Internal and external communication strategies ensure stakeholders are informed promptly and accurately during incidents.

This comprehensive approach not only addresses the immediate threat but also strengthens BC Ferries' long-term cybersecurity posture by continuously improving response capabilities and defense mechanisms against evolving ransomware threats.

# Preparation

The objective of this step is to ensure that the organization is ready to detect, respond to, and recover from a ransomware attack, minimizing downtime and impact.

## Incident Response Policies

For the purpose of protecting valuable assets, whether physical or information technology (IT) assets related, we have developed three incident response policies These policies help ensure confidentiality, integrity and availability (known as the CIA triad), while protecting sensitive customer data and personally identifiable information (PII) of the company, i.e. BC Ferries in support of a ransomware attack. [Ben Lutkevich, January 2025]

### Malware Detection Response Policy

**Purpose**: This policy outlines the procedures and actions required to contain, eradicate, and recover from ransomware attacks, minimizing the impact on the organization's operations, safeguarding critical data, and ensuring swift restoration of services.

**Policy Statement**:
The goal of this policy is to minimize the operational, financial, and reputational impact of ransomware incidents by ensuring that proper containment, eradication, and recovery procedures are followed. The policy is activated in the event of a malware being detected which is the first step of defence against ransomware.

**Scope**:
This policy applies to:
All employees, contractors, and third-party service providers who have access to the organization's systems, networks, and data.
All systems, devices, applications, and data managed or owned by the organization, including workstations, servers, and cloud-based environments.
Any individuals or departments involved in the identification, response, containment, eradication, and recovery efforts in the event of a ransomware attack.

**Procedure/ Responsibilities**:

- Employees
    - Follow proper cybersecurity protocols, including identifying and reporting suspicious emails, attachments, and links.
    - Do not attempt to resolve ransomware infections independently or bypass containment procedures.
- Managers
    - Ensure that all team members are aware of the policy and trained to recognize ransomware attack indicators.

    - Act as a liaison between employees and IT/security teams to facilitate rapid communication during an attack.
- Network/Security Team
    - Lead the response efforts during a ransomware attack, including isolating infected systems, performing malware eradication, and restoring systems from backups.
    - Ensure that incident documentation is completed, including root cause analysis and post-incident review.
    - Regularly update and patch systems to prevent vulnerabilities that could be exploited by ransomware.
- Communications Team
    - Coordinate the organization's response efforts in case of an attack, ensuring compliance with the incident response plan.
    - Facilitate communication with external experts, law enforcement, or cybersecurity agencies, as needed.
- Law/Compliance Team
    - Ensure that all legal and regulatory reporting requirements are met, including notifying relevant authorities, customers, and affected individuals if necessary.
    - Assess any legal ramifications related to the ransomware attack, including data breach implications.

**Compliance and Enforcement:**

Enforcement:

- Monitoring and Auditing - Compliance with this policy will be monitored through regular audits, vulnerability assessments, and penetration testing to identify gaps and areas for improvement.
- Incident Reporting - All employees and contractors must report suspected or confirmed ransomware incidents immediately according to the incident reporting process outlined by IT/security teams.

Consequences of Non-Compliance:

- Failure to Follow Procedures - Employees or managers who fail to adhere to this policy or fail to report an incident may be subject to disciplinary action, including termination, depending on the severity of the violation.
- Accountability - Employees who deliberately or negligently contribute to a ransomware incident (e.g., through poor cybersecurity hygiene or ignoring security protocols) may face sanctions, including loss of access to IT resources, retraining, or legal actions if applicable.

Policy References:


- NIST Special Publications 800-61v2 [August, 2012]
- SANS - Security Policy Templates [November, 2022]

## Data Breach Management Policy

**Purpose**: The purpose of this policy is to establish clear and effective procedures for identifying, containing, and notifying stakeholders when a breach involving Personally Identifiable Information (PII) occurs. The policy aims to protect the confidentiality, integrity, and availability of PII by ensuring a prompt and coordinated response to data breaches.

**Policy Statement**:
This policy intends to ensure that all data breaches involving PII are handled swiftly, transparently, and in compliance with applicable legal, regulatory, and organizational requirements. The organization is committed to safeguarding PII, minimizing the impact of breaches, and ensuring timely notifications to impacted individuals, regulatory bodies, and other relevant stakeholders by activating the policy as soon as a data breach is identified. The goal is to protect privacy rights, mitigate risks, and prevent reputational harm.

**Scope**:
This policy applies to:
All employees, contractors, and third-party vendors who have access to or manage PII in the organization.
All systems, networks, databases, and services that store, process, or transmit PII.
Any situation where a breach of PII is suspected, detected, or confirmed, regardless of the scale of the incident.
This policy applies at all levels of the organization and must be followed by all individuals with access to PII, including those in IT, legal, compliance, customer service, and other relevant departments.

**Procedure/ Responsibilities**:

- Employees:
    - Report any suspected or confirmed data breaches involving PII to their direct supervisor or the designated Data Protection Officer (DPO) immediately.
    - Cooperate with the investigation and containment process.
    - Follow security protocols for handling PII and preventing data breaches.
- Managers:
    - Ensure that employees are aware of and comply with the policy and procedures for reporting and responding to data breaches.
    - Take immediate action to assist in the containment and investigation of any potential data breaches.
    - Ensure proper communication to impacted stakeholders.
- Forensic Analyst:
    - Lead the investigation of data breaches involving PII, including identifying the source and scope of the breach.

    - Determine whether the breach meets the threshold for legal or regulatory notification requirements.
    - Oversee the containment and recovery efforts, ensuring minimal damage to PII.
- IT and Security Teams:
    - Immediately assess the breach, determine how PII was compromised, and implement containment measures.
    - Work to prevent further unauthorized access to PII by implementing technical solutions such as system isolation, password resets, or access revocation.
    - Support recovery efforts and ensure that systems are secured before returning to normal operation.
- Legal /Compliance Team:
    - Ensure compliance with data protection laws and regulations, including assessing the breach's legal implications and determining notification timelines.
    - Assist with notifying regulatory bodies, customers, and other parties as required.
    - Provide guidance on managing potential legal risks related to the breach.

**Compliance and Enforcement**:
Enforcement:

- All employees are required to comply with the terms of this policy. The organization will regularly audit compliance with data protection protocols to ensure adherence.
- Non-compliance with reporting or containment procedures may result in disciplinary actions, including termination, depending on the severity of the failure.

Consequences for Non-Compliance:

- Failure to Report - Employees who fail to report a suspected breach in a timely manner may be subject to disciplinary action, including but not limited to retraining, suspension, or termination.
- Failure to Contain or Mitigate - Employees who do not act promptly to contain or mitigate the breach may be held accountable for the extent of the damage.
- Delays in Notification - Delays in notifying affected individuals, regulatory bodies, or third parties, when required by law, may result in legal consequences for the organization and individuals involved.

Policy References:

- NIST Special Publications 800-61v2 [August, 2012]
- SANS - Security Policy Templates [November, 2022]

## Incident Log Retention Policy

**Purpose**: The purpose of this policy is to establish guidelines for the retention, review, and analysis of system and security logs within the organization. This policy ensures that logs are retained for at least 12 months, reviewed weekly for anomalies, and used for immediate forensic analysis during security incidents to support detection, investigation, and response efforts.

**Policy Statement**:
This policy aims to ensure that the organization maintains an effective log management strategy to enhance security, compliance, and incident response. By retaining logs for a minimum of 12 months and regularly analyzing them, the organization can identify trends, detect potential threats, and respond to incidents more effectively. Logs will also be available for forensic analysis when needed to understand the scope and impact of security events.

**Scope**:
This policy applies to:
All employees, contractors, and third-party vendors who have access to or manage the organization's IT infrastructure and systems that generate logs.
All systems, devices, applications, networks, and services that generate or rely on logs for security, operational, or compliance purposes, including servers, workstations, firewalls, routers, and security systems.
The IT department, security team, and incident response teams responsible for managing, reviewing, and analyzing logs.
This policy applies at all times, including during routine system operation and in the event of security incidents.

**Procedure/ Responsibilities**:

- Employees:
    - Ensure logs are properly generated by systems and applications under their control, following organizational standards.
    - Report any issues related to log generation, retention, or analysis to the IT or security teams.
- Managers:
    - Ensure that their teams are aware of and adhere to the log retention and analysis requirements outlined in this policy.
    - Support IT and security teams by providing necessary access to systems for log collection, retention, and analysis.
- IT and Security Teams:
    - Implement and manage the log retention infrastructure, ensuring that logs are retained for 12 months and that systems are in place for weekly reviews.
    - Perform weekly log reviews to identify potential security risks, vulnerabilities, or irregular activities.

    - Provide immediate forensic analysis and detailed reports during security incidents to assist in threat detection, response, and post-incident reviews.
- Incident Manager:
    - Access, review, and analyze logs during security incidents to determine the scope, timeline, and nature of the attack.
    - Cooperate with IT and security to ensure logs are preserved and securely stored for investigation.

**Compliance and Enforcement**:
Enforcement:

- Compliance with this policy will be regularly monitored by IT and security teams to ensure that logs are properly retained, reviewed, and analyzed as required.
- Non-compliance with log retention and review procedures will be identified through regular audits, and corrective actions will be taken.

Consequences for Non-Compliance:

- Failure to Retain Logs: Employees or teams who fail to retain logs according to this policy may face disciplinary action, including retraining or more severe measures, depending on the extent of the non-compliance.
- Failure to Review Logs: Teams or individuals who fail to review logs regularly or respond to potential security issues detected in logs may be subject to disciplinary actions or performance reviews.
- Failure to Analyze Logs During Incidents: Failure to conduct timely forensic analysis during a security incident could result in a failure to detect a breach, which could result in legal and reputational damage for the organization. Employees responsible for such lapses may face disciplinary measures, including suspension or termination.

Policy References:

- NIST Special Publications 800-61v2 [August, 2012]
- SANS - Security Policy Templates [November, 2022]
- CIS Critical Security Controls® Version 8.1 [August 2024]

## CSIRT Team

One of the key skills that a cyber Incident Response (IR) team needs to have in order to effectively respond to a ransomware attack is a deep understanding of how this type of malware and threat actors work. [Truesec, January 2023]

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

Below are details about the roles and responsibilities of each member of BC Ferries starting from to prevent and respond to a workplace incident:

| Member | Role | Responsibilities |
|---|---|---|
| Internal Stakeholders | | |
| James Tan | CIO | Responsible for reporting to board directors and other executives. Also, making decisions on the best way forward based on information provided by members of the CSIRT team. |
| Skip Sheffield | Incident Manager | Setting priorities and making decisions regarding the response to a security breach, developing response plans, coordinating with other teams and stakeholders, and reporting on the progress of the response. |
| Prinson D'silva | Security Analyst | Monitoring the organization's networks and systems for suspicious activity and identifying security incidents as they occur and ensure the response delivery is timely and effective. |
| George Corcoran | IT/ Network Administrator | Managing and maintaining the organization's networks, configuring security controls, monitoring network traffic, and implementing network segmentation. |
| James Rodrigues | Communications Expert | They are the messenger to ensure that internal/external stakeholders, customers, and the public are informed in a timely and compliant fashion. |
| Denise Coffey | Law/ Compliance Officer | Reviews regulatory and legal obligations, handles notifications to authorities and affected individuals (if required), and oversees compliance with data protection laws. |
| Mike Ogunlaja | Forensic Analyst | Performs forensic analysis of infected systems to determine how the attack occurred, whether data was exfiltrated, and provides detailed evidence of the breach. |
| External Stakeholders | | |
| Cybersecurity Vendor Pvt. Ltd. | Network Security Vendor | Baseline Cyber Security Controls for large Organizations. |
| Ransomware Decryptor Inc. | Ransomware Decryption Service Provider | Provides assistance in case no backups or decryptors are available. |
| Vancouver Police Department (VPD) | Law Enforcement (local) | Cybercrime Reporting and escalation to federal division if required. |

Along with these, the Preparation step includes a few additional practices such as:

- Conduct exercises, drills regularly
- Test the plan, team and tools
- Established service-level agreement (SLA), response times

## Detection and Analysis

The objective of this step is to detect the ransomware attack quickly, determine its scope, and analyze its impact.

According to NIST, some of the common attacks methods are:

- Email attachments and embedded malicious links
- Web browser vulnerabilities
- Infected programs bundled with malware
- Portable USB devices

### Initial Incident Triage

As the first line of defence, Prinson D'silva will be responsible for investigation and detection of the incident based on the following trigger points:

- Unusual File Changes: Files are encrypted and the file extensions change (e.g., .locked, .encrypted).
- Ransomware Note: A ransom note appears on infected systems, demanding payment.
- Suspicious Network Activity: Unusual communication with external servers (e.g., C2 servers).
- Alerts from Security Tools: IDS/IPS or endpoint detection systems flag potential ransomware activity.
- Employee Reports: Employees notice slow system performance or are unable to access files.

Based on the trigger points, the following questions would be asked during the initial investigation:

- Is the attack confirmed to be ransomware (e.g., files are encrypted, ransom note found)?
- How widespread is the attack? Is it affecting specific systems or the entire network?
- Have any critical systems been impacted (e.g., payment systems, operational systems)?
- What is the ransom demand, and are there any indications of data exfiltration?

Escalation Points: If any of the following are true:

- If the ransomware has encrypted critical systems or data:

    - Escalate to Skip Sheffield and initiate full CSIRT activation.
- If data exfiltration is suspected or confirmed:
    - Escalate to Denise Coffey for data breach notifications.

### Incident Severity Matrix

According to the Incident Severity Matrix provided by the Innovation, Science and Economic Development Canada [2021], the Severity of the Incident will be determined.

| Category | Indicators | Scope | Action |
|---|---|---|---|
| 1 – Critical | Data loss, Malware | Widespread and/or with critical servers or data loss, stolen data, or unauthorized data access | Implement CSIRT, Incident Response Plan, create Cyber Security Incident, Organization-wide |
| 2 – High | Theoretical threat becomes active | Widespread and/or with critical servers or data loss, stolen data, or unauthorized data access | Implement CSIRT, Incident Response Plan, create Cyber Security Incident, Organization-wide |
| 3 – Medium | Email phishing or active spreading infection | Widespread | Implement CSIRT, Incident Response Plan, create Security Incident, Organization-wide |
| 4 - Low | Malware or phishing | Individual host or person | Notify CSIRT, create Cyber Security Incident |

Based on the nature of our attack and given the indicators and scope, this incident is categorized as Critical as we further escalate this to other Members of the CSIRT team.

## Containment, Eradication, and Recovery

In this step, the goal of the CSIRT team is to contain the attack to prevent further damage, eradicate the ransomware, and recover affected systems.

### Incident Response Playbook

This is the step where we Implement the incident response playbook.
The following steps would be followed by Prinson:

### Containment Measures

- Ensure reported information is factual based on evidence available at the time.
- Ensure a point of contact knows the current status at all times.
- Prevent further damage by containing the incident.
- Determine the source, what vulnerability was exploited and implement repairs.
- Determine what was changed (for example, files, connections, processes, accounts, access).
- Acquire, preserve, secure and document evidence and preserve the chain of custody.
- Continue taking notes, ensuring a detailed log about what was found and what you did about it.
- Disconnect devices identified with ransomware from the network immediately.
- Examine the ransomware and establish how it infected the device. This will help you to understand how to remove it from the device.

### Other Containment Measures:

In the event that Prinson requires help with containment, contact George Corcoran for network isolation as well as Cybersecurity Vendor Pvt. Ltd. to help with additional expertise conducting the following steps:

- Disconnect devices identified with ransomware from the network immediately.
- Examine the ransomware and establish how it infected the device. This will help you to understand how to remove it from the device.
- Disable VPNs, remote desktop protocols, or any other access points to prevent further spread.

### Eradication Measures

- Remove all traces of the infection or other incident
    - Identify and mitigate all vulnerabilities that were exploited
    - Remove malware, inappropriate materials, and other components
- If more affected hosts are discovered (for example, new malware infections), perform the identification steps on the newly identified examples, then contain
- Ensure the incident cannot re-occur
- Further understand the attack method and exploited vulnerabilities
- Continue taking notes, ensuring a detailed log
- Ensure any compromised machines are removed or formatted before placing back into service
    - Ensure necessary evidence has been collected

### Other Eradication Measures:

In the event that Prinson requires help with eradication, contact Ransomware Decryptor Inc. to help with additional expertise conducting the following steps:

- Identify the Ransomware Variant: Use available tools to identify the ransomware variant and find solutions for decryption (e.g., from No More Ransom project).
- Remove the Ransomware: Perform a full malware scan on infected systems and remove any remaining traces of the ransomware. Ensure that all backdoors and persistence mechanisms are eliminated.
- Patch Vulnerabilities: Apply patches and security updates to systems that were exploited in the attack (e.g., unpatched RDP vulnerabilities).

### Recovery Measures

- Return affected systems to an operationally ready state one by one.
- Monitor closely to ensure the incident does not re-occur and is not still ongoing.
- Ensure systems are restored from a trusted source.
- Confirm the affected systems are functioning normally.
- Implement additional monitoring to look for future related activity if necessary.

### Other Recovery Measures:

In the event that Prinson requires help with recovery, contact George Corcoran for monitoring the network along with Cybersecurity Vendor Pvt. Ltd. to help with additional expertise conducting the following steps:

- Once the ransomware has been removed, a full system scan must be performed using the most up-to-date anti-virus, anti-malware, and any other security software available, to verify it has been removed from the device.
- If the ransomware cannot be removed from the device (as is often the case with rootkits) it should be rebuilt using original installation media or images. Prior to restoration from back-up media/images you must verify that the back-up media/images are not infected by malware.
- If data is critical and must be restored, but cannot be retrieved from unaffected backups, search available decryptors from nomoreransom.org
- Protect the system(s) to prevent further infection by implementing fixes and/or patches to prevent further attack.

### Communication - James Rogrigues:

- Contact local authorities (VPD) to report the incident and cooperate with their investigation
- Keep all internal stakeholders informed about recovery progress and any disruptions.
- If required, notify affected customers, partners, and regulatory bodies in accordance with legal obligations.

## Post-Incident Activity

This is the last step of the Incident Response Plan where the CSIRT team will Analyze the incident for lessons learned and improve the organization's defenses and

response capabilities.

## Post-Incident Review

Conduct a "Lessons Learned" Meeting: Bring together the CSIRT and key stakeholders to review the incident and assess the response process.

**Questions for the Review:**

- What was the cause of the ransomware infection? Was it preventable (e.g., unpatched software, phishing)?
- How effective were the detection and containment measures?
- Was the response time appropriate? Could actions have been taken faster or more efficiently to improve SLA?
- Were communication protocols effective, both internally and externally?

**Root Cause Analysis - Mike Ogunlaja:**

- Perform a root cause analysis to identify weaknesses in the organization's cybersecurity posture that allowed the ransomware to penetrate.
- Was the attack vector a phishing email, insecure remote access, or a vulnerability in software?
- Identify potential improvements in technical and administrative controls (e.g., stronger email filtering, multi-factor authentication, endpoint protection).

**Update Incident Response Plan - Skip Sheffield:**

- Revise the ransomware incident response playbook based on findings to improve future response efforts.
- Ensure that the CSIRT is properly trained on new tactics, techniques, and procedures (TTPs) used by ransomware actors.

**Enhance Security Posture - Skip Sheffield/ Prinson/ Cybersecurity Vendor Pvt. Ltd.:**

- Strengthen preventative measures, such as improving endpoint detection, network segmentation, and user awareness training.
- Implement stronger backup and recovery strategies, ensuring offline or air-gapped backups are in place.

**Monitor for Recurrence - Prinson:**

- Increase monitoring for indicators of ransomware re-infection (e.g., malicious file extensions, encrypted files).
- Implement more robust security controls to detect early signs of lateral movement or data exfiltration.

**Regulatory Reporting and Compliance - James Rodrigues/ Denise Coffey :**

- Ensure the incident is reported to regulatory bodies (e.g., PCI DSS, PIPEDA) within required timelines.
- Document the breach and ensure that all legal and compliance obligations are met.

## Conclusion & Recommendations

By following this playbook based on the NIST 4-step Incident Response Lifecycle, BC Ferries can effectively detect, contain, and recover from a ransomware incident. The CSIRT plays a critical role in coordinating efforts across departments, and the post-incident activities ensure the organization learns from the event and strengthens its defenses against future attacks.

According to the MITRE ATT&CK framework, here are some following key mitigations against ransomware attacks recommended for this incident response plan:

**Initial Access:**

- Mitigations: Email filtering, strong password policies, multi-factor authentication, user awareness training.
- Relevant Techniques: "Spear Phishing Attachment", "Phishing Link".

**Execution:**

- Mitigations: Application whitelisting, endpoint detection and response (EDR), script blocking.
- Relevant Techniques: "PowerShell", "Remote Services".

**Privilege Escalation:**

- Mitigations: Least privilege access controls, regular system patching.
- Relevant Techniques: "Local System Authority Bypass", "Exploit Public Facing Application".

**Data Exfiltration:**

- Mitigations: Network traffic monitoring, data loss prevention (DLP) solutions.
- Relevant Techniques: "Data Exfiltration over C2 Channel", "Exfiltration to Cloud Storage".

**Encryption:**

- Mitigations: Regular backups to an isolated system, data recovery procedures.
- Relevant Techniques: "Ransomware".

[Top ATT&CK Techniques, January 2025]

## References


- Paul Cichonski, Tom Millar, TimGrance, Karen Scarfone (August, 2012) - *Computer Security Incident Handling Guide* . NIST Special Publication 800-61 Revision 2. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- Matthew Kosinski (Retrieved January, 2025) - *What is ransomware?.* IBM. Retrieved from https://www.ibm.com/think/topics/ransomware
- Ben Lutkevich (Retrieved January, 2025) - *Security policy.* Tech Target. Retrieved from https://www.techtarget.com/searchsecurity/definition/security-policy
- SANS (November 2022) - *Security Policy Templates.* Retrieved from https://www.sans.org/information-security-policy/
- Center for Internet Security (August 2024) - *CIS Critical Security Controls® Version 8.1.* CIS. Retrieved from https://learn.cisecurity.org/cis-controls-v8-1-guide-pdf
- Cynet (January, 2025) - *Incident Response Plan Templates.* Retrieved from https://www.cynet.com/incident-response/incident-response-plan-template/
- Truesec (January, 2023) - *Skills Needed for an Efficient Cyber Incident Response Team.* Retrieved from https://www.truesec.com/hub/blog/ransomware-attacks-and-the-skills-needed-for-an-efficient-and-successful-cyber-incident-response-team
- Innovation, Science and Economic Development Canada (2021) - *Develop an Incident Response Plan.* Government of Canada. Retrieved from https://ised-isde.canada.ca/site/cybersecure-canada/en/certification-tools/develop-incident-response-plan-fillable-template-and-example
- MITRE ATT&CK (Retrieved January, 2025) - *Techniques > Enterprise.* MITRE. Retrieved from https://attack.mitre.org/
- Top ATT&CK Techniques (Retrieved January, 2025) - Ransomware Top 10 Techniques. MITRE Engenuity. Retrieved from https://top-attack-techniques.mitre-engenuity.org/#/