IR Plan, Playbook and Policy

Prepared by: Anastasiya Gruneva
Date: January 23rd, 2025

Table of Contents

Executive Summary....................3
Company's overview....................4
Incident Response Playbook: Ransomware....................6
Communications and Media Policy....................10
Incident Response Data Collection Policy....................13
Access Control Policy....................16
Slideshow....................19
References....................20

Executive Summary

Overview of Nova Scotia Power
Nova Scotia Power (NSP) is a critical electricity provider in Nova Scotia, serving 95% of the population, including residential, commercial, and industrial customers. Founded in 1919, it is a subsidiary of Emera Inc. and operates under the regulatory oversight of the Nova Scotia Utility and Review Board (UARB). With over 2,200 employees, NSP manages a diverse energy portfolio including hydroelectric, wind, coal, and natural gas facilities, along with an extensive grid infrastructure.

Key Stakeholders
NSP's operations engage a broad range of stakeholders, including residential and commercial customers, UARB regulators, parent company Emera Inc., shareholders, environmental advocacy groups, employees, and local communities. These stakeholders are integral to the company's operational and strategic decision-making.

Incident Response
To address potential risks such as ransomware attacks, power outages, and environmental incidents, NSP has implemented robust response policies and playbooks. The **Ransomware Incident Response Playbook**, based on NIST guidelines, provides a structured approach to preparing for, detecting, and responding to cybersecurity threats. Key elements include:

- **Preparation**: Employee training, regular system backups, and multi-factor authentication.
- **Detection and Analysis**: Real-time monitoring and escalation protocols.
- **Containment, Eradication and Recovery**: Isolation of affected systems, removal of malicious software, and restoration of clean backups.
- **Post-Incident Activity**: Root cause analysis, system hardening, and updating policies based on lessons learned.

Supporting Policies

- **Communications and Media Policy**: Ensures accurate and timely communication with stakeholders during incidents to protect NSP's reputation and comply with regulatory requirements.
- **Incident Response Data Collection Policy**: Provides standardized guidelines for collecting and preserving data during cybersecurity incidents, aiding forensic analysis and compliance.
- **Access Control Policy**: Establishes a framework for securing access to critical systems, reducing the risk of unauthorized access and safeguarding sensitive information.

This comprehensive approach underscores Nova Scotia Power's commitment to delivering reliable electricity while prioritizing security, sustainability, and stakeholder trust.

Company’s overview

Overview of Nova Scotia Power

Nova Scotia Power (NSP) is a leading electricity provider serving 95% of Nova Scotia’s population, including residential, commercial, and industrial customers. Established in 1919 and now a subsidiary of Emera Inc., the company operates as a regulated utility under the oversight of the Nova Scotia Utility and Review Board (UARB). Nova Scotia Power is vital to the province’s economic and social infrastructure, generating, transmitting, and distributing electricity to over 540,000 customers.

Organizational Structure and Size

Nova Scotia Power is a mid-sized utility company with a workforce of over 2,200 employees, encompassing a wide range of functions such as power generation, grid maintenance, customer service, environmental compliance, and administration. Its organizational structure includes executive leadership (e.g., CEO, CFO, CIO), operational departments (e.g., engineering, environmental services, IT), and field workers. The company operates a network of power plants, including hydroelectric, wind, coal, and natural gas facilities, along with a robust grid infrastructure that spans the province. (Nova Scotia Power, 2025)

Industry

Nova Scotia Power operates in the energy and utilities sector, which is highly regulated and vital for public services. The company is committed to transitioning toward renewable energy, with initiatives to reduce greenhouse gas emissions and expand wind and solar energy production. As part of the broader energy transition, NSP is subject to stringent environmental standards and carbon reduction mandates.

Key stakeholders attached to Nova Scotia Power:

1. Customers – Residential, commercial, and industrial consumers who depend on Nova Scotia Power for reliable electricity.
2. Nova Scotia Utility and Review Board (UARB) – The provincial regulator responsible for overseeing utility operations, approving rates, and ensuring compliance with regulations.
3. Emera Inc. – The parent company of Nova Scotia Power, which oversees its financial and operational performance.
4. Shareholders of Emera Inc. – Investors who have a financial interest in Nova Scotia Power’s profitability and sustainability.
5. Chief Executive Officer (CEO) – The top executive responsible for the company’s overall strategy, decision-making, and accountability.

6. Chief Information Officer (CIO) – Oversees IT operations and cybersecurity to protect infrastructure and customer data.
7. Environmental Advocacy Groups – Organizations monitoring Nova Scotia Power's environmental practices, emissions, and renewable energy initiatives, such as the Ecology Action Centre.
8. Employees – Including field technicians, engineers, customer service representatives, and executive leadership.
9. Local Communities – Municipalities and residents affected by the company's operations, from power outages to renewable energy projects.

Examples of specific incidents:

- Power outages: Directly impact customers, operations, and public safety.
- Cybersecurity breaches: Could disrupt smart grid systems, expose customer data, and cause widespread operational failure.
- Environmental spills: Impact the company's reputation, regulatory compliance, and the environment.
- Equipment failure or workplace accidents: Affect employee safety and service reliability.

Incident response plans must prioritize minimizing customer impact, restoring services quickly, and addressing safety risks. The severity of the incident dictates whether internal departments, customers, regulators, or the media are informed.

Internal incidents might only involve HR or IT teams, while external or industry-specific incidents could involve emergency services, customers, government bodies, and media.

Incident Response Playbook: Ransomware

Objective
To outline a detailed workflow and assign roles and responsibilities for responding to a ransomware incident impacting Nova Scotia Power, ensuring minimal disruption to operations and swift remediation.

Workflow Steps
The steps come from NIST Computer Security Incident Handling Guide (NIST, 2025).

Step 1: Preparation

Establish readiness to prevent and respond to ransomware incidents.

Actions:

1. Policy and Procedures: Establish and regularly update a ransomware response policy that outlines response steps, communication plans, and decision-making protocols.
2. Employee Training: Conduct mandatory cybersecurity training, focusing on identifying phishing emails, secure password practices, and ransomware prevention. Reference: Communications and Media Policy for guidelines on messaging during training and incidents.
3. Backup Strategy: Ensure all critical systems and data are backed up regularly, and backups are stored offline or in immutable storage. Test backup restoration regularly.
4. Incident Response Team (IRT): Maintain an IRT that includes members from IT, cybersecurity, legal, communications, HR, and executive leadership. Define clear roles and responsibilities.
5. Threat Intelligence: Subscribe to threat intelligence feeds to stay informed about ransomware tactics and trends.
6. Access Control: Implement least privilege access and multi-factor authentication (MFA) across all systems.

Step 2: Detection and Analysis

Detect and confirm ransomware incidents using industry best practices.

Trigger Items:

- Unusual file encryption activities or unauthorized file modifications (MITRE: T1486, 2025).
- Detection of known ransomware signatures or indicators of compromise (MITRE: T1078, 2025).
- Unexpected network traffic patterns suggesting data exfiltration (MITRE: T1020, 2025).
- User reports of inaccessible files or the presence of ransom notes.
- Security tool alerts (e.g., antivirus, EDR) indicating ransomware-related activities.
- SOC notifications of detected anomalies.

Trigger Points (Questions):

- Are critical files or systems suddenly inaccessible?
- Does the organization need to engage 3rd party technical resources to help with the incident?

Actions:

1. Monitor for unusual system behaviors, such as encryption of files or unauthorized access attempts. Logs should be collected and analyzed following the Incident Response Data Collection Policy.
2. Determining the legitimacy of the ransomware attack.
3. Identify the Scope: Determine the affected systems, data, and network segments.
4. Containment Decision: Decide on immediate containment actions (e.g., disconnect affected devices from the network).
5. Alert Notifications: Notify the IRT, CIO, and affected departments.
6. Preserve Evidence: Capture memory dumps, log files, and network traffic for forensic analysis.
7. Classify the Incident: Use the severity matrix to assess the business impact and prioritize response efforts.

Responsibilities:

- IT Security Lead: Analyze alerts and investigate the scope of the ransomware incident.
- System Administrators: Verify affected systems and assist with containment efforts.
- CIO: Approve escalations and oversee the coordination of resources.
- IRT Members: Communicate findings and coordinate immediate actions.

Escalations:

- If critical infrastructure is affected, escalate to the executive team and the regulatory liaison.
- Notify external partners (e.g., third-party cybersecurity consultants) if the situation exceeds internal capabilities.

Step 3: Containment, Eradication and Recovery

Prevent the spread of ransomware across systems.

Immediate Actions:

1. Isolate affected systems to prevent lateral movement.
2. Block known malicious IPs and domains.
3. Disable compromised accounts.
4. Notify stakeholders and follow guidelines outlined in the Communications and Media Policy for internal and external communication.

Eradication:

1. Identify and remove ransomware payloads using forensic analysis.
2. Patch vulnerabilities exploited by the attackers.
3. Reset credentials for compromised accounts.

Recovery:

1. Restore systems and data from clean backups.
2. Verify integrity of recovered data.
3. Gradually reconnect systems to the network and monitor closely.

Trigger Points (Questions):

- Have all affected systems been identified and isolated?
- Do any third-parties or government agencies need to be notified?
- Are any customer communications required?

Responsibilities:

- IT Security Lead: Lead containment efforts and coordinate technical actions.
- Network Administrators: Update firewalls, segment networks, and monitor traffic.
- IRT Coordinator: Ensure all team members are aligned on containment actions. Document recovery progress and update stakeholders.
- Backup Team: Ensure backups are accessible and malware-free.
- IT Team: Validate and restore system functionality.

Escalations:

- Notify external cybersecurity experts if containment measures fail.
- Escalate to the CEO and legal counsel if regulatory reporting is required.
- Escalate to the Public Relations Lead if communication with external stakeholders and media is required.

Communication:

- Internal Communication: Provide regular updates to employees and the executive team.
- External Communication: Notify affected customers, regulators (UARB), and other stakeholders as required by law.
- Media Handling: Work with public relations to issue transparent and consistent statements.

Step 4: Post-Incident Activity

After the incident, conduct a detailed review to identify lessons learned and improve preparedness.

Actions:

1. Incident Report: Document the timeline, root cause, containment, and recovery actions.
2. Post-Mortem Review: Organize a meeting with the IRT to analyze: what went well, areas for improvement, recommended changes to policies and procedures.
3. System Hardening: Implement security patches, updates, and additional safeguards identified during the incident.
4. Training: Conduct targeted training sessions based on incident findings.
5. Metrics: Track and report on key performance indicators (KPIs): time to detect (TTD), time to contain (TTC), time to recover (TTR), financial and reputational impact.
6. Update security policies and procedures, including the Access Control Policy, Incident Response Data Collection Policy, and Communications and Media Policy, based on lessons learned.

Responsibilities:

- IRT Coordinator: Compile the incident report and oversee post-mortem reviews.
- Training Lead: Update training materials and schedule sessions.
- Executive Leadership: Review post-incident findings and approve resource allocation for improvements.

Communications and Media Policy

1. Purpose of the Policy

The Communications and Media Policy is designed to establish a standardized framework for managing internal and external communications during cybersecurity incidents, including ransomware attacks (NIST Computer Security Incident Handling Guide, 2025). The primary objectives are to ensure accurate, consistent, and timely communication, protect Nova Scotia Power's reputation, and comply with legal and regulatory requirements.

2. Importance of the Policy

From a security perspective, effective communication during a cybersecurity incident is critical to:

- Prevent the spread of misinformation that could escalate public concern or damage trust.
- Minimize operational disruption by ensuring all stakeholders receive clear instructions.
- Protect sensitive company and customer data by controlling the release of information.
- Comply with regulatory requirements and avoid penalties for miscommunication or lack of reporting (UARB Incident Reporting and Response, 2025).
- Preserve the company's reputation and maintain public confidence.

3. Activities, Frequency, and Responsibilities

a) Pre-Incident Preparation

- Activity: Develop communication templates (e.g., incident notification, press releases, internal memos).
  Frequency: Annually and as needed.
  Responsibility: Corporate Communications Team in collaboration with the Incident Response Team (IRT).

- Activity: Identify and train spokespersons (e.g., CEO, CIO, PR lead).
  Frequency: Semi-annually.
  Responsibility: HR and Communications Departments.

- Activity: Establish a stakeholder communication matrix (e.g., customers, regulators, media).
  Frequency: Quarterly review and updates.

Responsibility: Communications and Regulatory Affairs Teams.

b) During an Incident

- Activity: Activate the communications plan outlined in the Ransomware Incident Response Playbook.
  Frequency: As soon as the incident is identified.
  Responsibility: Incident Response Coordinator and Communications Lead.
- Activity: Deliver consistent messages to stakeholders (e.g., customers, employees, regulators).
  Frequency: As per incident severity and updates.
  Responsibility: Corporate Communications Team and designated spokespersons.
- Activity: Coordinate press releases and media responses.
  Frequency: As needed, aligned with the incident timeline.
  Responsibility: Public Relations Lead.
- Activity: Notify regulatory authorities (e.g., Nova Scotia Utility and Review Board) and customers as required.
  Frequency: Within legally mandated timeframes.
  Responsibility: Regulatory Affairs Team.

c) Post-Incident Activities

- Activity: Conduct a post-mortem analysis of communication strategies used.
  Frequency: Within 30 days post-incident.
  Responsibility: Incident Response Team and Communications Team.
- Activity: Update communication plans and templates based on lessons learned.
  Frequency: As part of post-incident reporting.
  Responsibility: Corporate Communications Team.

4. Related Playbook and Usage

This policy is directly linked to the Ransomware Incident Response Playbook, which will be used to:

- Trigger activation of the communications plan during ransomware incidents.
- Provide a clear escalation matrix for communication decisions.
- Guide messaging strategies to internal and external stakeholders.
- Ensure regulatory compliance for incident reporting.

5. Consequences of Non-Compliance

Individual Consequences:

- First Violation: Formal warning and mandatory training on the Communications and Media Policy.
- Repeat Violations: Disciplinary action, up to and including termination of employment, depending on severity.
- Severe Breaches: Legal consequences if actions result in data breaches or regulatory violations.

Organizational Consequences:

- Reputational Damage: Loss of public trust and customer confidence.
- Regulatory Penalties: Fines or sanctions from regulatory bodies for non-compliance with reporting requirements.
- Operational Disruption: Increased confusion and delays in incident containment and recovery.
- Legal Liability: Potential lawsuits from stakeholders due to inadequate communication.

Incident Response Data Collection Policy

1. Purpose of the Policy

The Incident Response Data Collection Policy aims to establish a standardized approach to gathering, storing, and analyzing data during cybersecurity incidents. This ensures effective incident response, supports forensic investigations, and aids in compliance with legal and regulatory obligations (NIST Computer Security Incident Handling Guide, 2025).

2. Importance of the Policy

From a security perspective, this policy is critical because:

- Supports Incident Containment and Recovery: Accurate data collection allows for precise identification of compromised systems and enables quicker containment and recovery.
- Facilitates Forensic Investigations: Properly collected data provides evidence to determine the root cause of incidents and prevent recurrence.
- Ensures Compliance: Adhering to data collection standards ensures compliance with regulatory requirements and avoids legal consequences (UARB Incident Reporting and Response, 2025).
- Preserves Organizational Integrity: Controlled data handling minimizes the risk of data leaks and maintains stakeholder trust.

3. Activities, Frequency, and Responsibilities

a) Pre-Incident Preparation

- Activity: Define data collection requirements (e.g., logs, network traffic, user activity).
  Frequency: Annually and after significant system changes.
  Responsibility: IT Security Team in collaboration with the Incident Response Team (IRT).

- Activity: Establish and configure centralized logging and monitoring systems.
  Frequency: Reviewed quarterly.
  Responsibility: IT Operations and Security Teams.

- Activity: Train relevant staff on data collection tools and techniques.
  Frequency: Semi-annually.
  Responsibility: HR and IT Security Teams.

b) During an Incident

- Activity: Collect data from affected systems (e.g., logs, snapshots, memory dumps).
  Frequency: Immediately upon incident detection.
  Responsibility: Incident Response Team and IT Security Team.

- Activity: Preserve data integrity using secure storage and hashing techniques.
  Frequency: Throughout the incident response process.
  Responsibility: Forensics Lead.

- Activity: Document all data collection activities in the incident log.
  Frequency: In real time during incident response.
  Responsibility: Incident Response Coordinator.

c) Post-Incident Activities

- Activity: Analyze collected data to identify root causes and vulnerabilities.
  Frequency: During post-incident reviews.
  Responsibility: Forensics Team and Incident Response Team.

- Activity: Archive collected data securely for future reference and compliance.
  Frequency: Within 30 days post-incident.
  Responsibility: IT Security Team.

- Activity: Update data collection procedures based on lessons learned.
  Frequency: After each post-incident review.
  Responsibility: IT Security and Incident Response Teams.

4. Related Playbook and Usage

This policy is directly linked to the Ransomware Incident Response Playbook, which provides:

- Guidelines on initiating data collection processes during ransomware incidents.
- Clear instructions for ensuring data integrity and proper documentation.
- Steps for analyzing collected data to support incident containment and root cause analysis.

5. Consequences of Non-Compliance

Individual Consequences:

- First Violation: Formal warning and mandatory training on data collection procedures.
- Repeat Violations: Disciplinary action, up to and including termination of employment, depending on severity.
- Severe Breaches: Legal consequences if actions result in regulatory violations or compromised forensic investigations.

Organizational Consequences:

- Operational Impact: Delayed incident containment and recovery due to insufficient data.
- Reputational Damage: Loss of stakeholder trust and customer confidence.
- Regulatory Penalties: Fines or sanctions from regulatory bodies for non-compliance with incident reporting requirements.
- Legal Liability: Potential lawsuits due to mishandling or loss of critical data.

Access Control Policy

1. Purpose of the Policy

The Access Control Policy establishes a framework for managing and securing access to Nova Scotia Power's (NSP) systems, applications, and facilities. Its primary goal is to ensure that only authorized individuals have access to sensitive information and resources, reducing the risk of unauthorized access and potential breaches.

2. Importance of the Policy

From a security perspective, this policy is essential because:

- Prevents Unauthorized Access: Controls access to sensitive data, reducing the risk of data breaches and insider threats (NIST Security and Privacy Controls for Information Systems and Organizations, 2025).
- Protects Critical Infrastructure: Secures systems and facilities critical to the delivery of electricity to customers, ensuring continuity of service.
- Supports Regulatory Compliance: Meets industry and government regulations, such as UARB and Canadian cybersecurity mandates, ensuring the organization avoids penalties and maintains trust.
- Preserves Confidentiality, Integrity, and Availability: Safeguards the organization's information assets, minimizing operational disruptions and reputational damage.

3. Activities, Frequency, and Responsibilities

a) Pre-Implementation Activities

- Activity: Define access control roles and permissions based on the principle of least privilege.
  Frequency: Annually and when new systems or roles are introduced.
  Responsibility: IT Security and Human Resources Teams.

- Activity: Implement multi-factor authentication (MFA) for all critical systems.
  Frequency: Reviewed semi-annually for effectiveness.
  Responsibility: IT Security Team.

- Activity: Conduct background checks on employees and contractors before granting access to sensitive systems.
  Frequency: For all new hires and contractors.

Responsibility: Human Resources and Compliance Teams.

b) Operational Activities

- Activity: Monitor and log access to systems and applications.
  Frequency: Continuous, with logs reviewed weekly.
  Responsibility: IT Operations and Security Teams.

- Activity: Perform regular access reviews to ensure access rights align with job responsibilities.
  Frequency: Quarterly.
  Responsibility: Department Managers and IT Security Team.

- Activity: Revoke access immediately upon employee or contractor termination.
  Frequency: Within 24 hours of termination.
  Responsibility: Human Resources and IT Security Teams.

c) Post-Incident Activities

- Activity: Audit access logs following security incidents to identify unauthorized access.
  Frequency: After each security incident.
  Responsibility: Incident Response Team and IT Security Team.

- Activity: Update access control policies based on lessons learned.
  Frequency: After post-incident reviews.
  Responsibility: IT Security and Compliance Teams.

4. Related Playbook and Usage

This policy is directly linked to the Incident Response Playbook and Ransomware Incident Response Playbook. These playbooks outline:

- Steps for identifying unauthorized access during incidents.
- Guidelines for revoking compromised credentials.
- Procedures for restoring access after containment.

5. Consequences of Non-Compliance

Individual Consequences:

- First Violation: Formal warning and mandatory security awareness training.

- Repeat Violations: Revocation of access privileges, disciplinary actions, or termination.
- Severe Breaches: Legal consequences if non-compliance results in data breaches or regulatory violations.

Organizational Consequences:

- Operational Impact: Increased risk of unauthorized access, leading to disruptions and potential outages.
- Regulatory Penalties: Fines or sanctions from regulatory bodies for non-compliance.
- Reputational Damage: Loss of customer and stakeholder trust due to perceived negligence.
- Financial Loss: Increased costs related to incident response and remediation.

Slideshow

A slideshow that announces Policies to Nova Scotia Power:

https://docs.google.com/presentation/d/1emfd4PaiLxjNq14oyBQ3u5ZlQGJkGchBpOuL-5wP6NQ/edit?usp=sharing

References

Nova Scotia Power, website (retrieved 2025, January 23) https://www.nspower.ca/

NIST Computer Security Incident Handling Guide (retrieved 2025, January 23)
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

NIST Security and Privacy Controls for Information Systems and Organizations (retrieved 2025, January 23)
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

MITRE ATT&CK (retrieved 2025, January 23) https://attack.mitre.org/

Nova Scotia Utility and Review Board (UARB) Incident Reporting and Response Planning (retrieved 2025, January 23)
https://www.nerc.com/pa/stand/reliability%20standards/cip-008-6.pdf