LIGHTHOUSE LAB

CYBERSECURITY

NOVA SCOTIA POWER IR PLAN, PLAYBOOK AND POLICY

OLADAPO OLUWAYALE

Table of Contents Page

Executive Summary

Cybersecurity incidents are a growing concern for utility companies like Nova Scotia Power (NSP), which manages essential infrastructure such as power generation, transmission, and distribution systems. Given its critical role in providing electricity to Nova Scotia, NSP must prioritize the protection of its systems from cyber threats. "The increasing sophistication, frequency and scale of cyber-related incidents has created an immediate need for Nova Scotia Power to advance security countermeasures," the company wrote in its filing to the Nova Scotia Utility and Review Board. (CBC News, 2019)

This Ransomware Incident Playbook outlines a structured approach for Nova Scotia Power (NSP) to respond effectively to a ransomware attack. Nova Scotia Power Incorporated (NSPI) recognizes the importance of protecting our customers' privacy. (Nova Scotia Power, n.d.) Given NSP's reliance on an internal Security Operations Center (SOC) and an outsourced Managed Security Service Provider (MSSP), the playbook ensures a coordinated, timely, and efficient response across both teams, minimizing operational and financial impact.

The playbook is organized into six key incident response phases:

1. **Preparation**: Ensures that both internal and external resources are ready to respond, with a focus on regularly tested backups, training, and a clear escalation matrix.
2. **Detection**: Leverages advanced security tools (e.g., SIEM, EDR) and MSSP expertise to quickly identify ransomware indicators and confirm the scope of the attack.
3. **Containment**: Rapidly isolates affected systems, preventing further spread of the ransomware across NSP's IT and OT environments, with collaborative input from both SOC and MSSP.
4. **Eradication**: Removes ransomware from infected systems, leveraging the MSSP's experience to ensure complete eradication, and restores clean backups where possible.
5. **Recovery**: Focuses on restoring critical systems and services, conducting integrity checks, and continuously monitoring for any residual threats.
6. **Lessons Learned**: After the incident, a thorough review is conducted to identify weaknesses, improve security posture, and refine response strategies for future attacks.

The playbook also includes communication protocols for internal and external stakeholders, ensuring that all parties—employees, customers, regulatory bodies, and law enforcement—are informed throughout the process. Key ransomware-specific considerations are addressed, including the decision-making process for ransom payments and decryption tool use, alongside legal and regulatory compliance requirements.

By following this playbook, NSP ensures a well-coordinated response to ransomware threats, minimizing downtime, ensuring legal compliance, and enhancing overall resilience against future attacks.

1. Introduction

Purpose:

The purpose of this playbook is to guide Nova Scotia Power through the various phases of responding to a ransomware incident. Given NSP's reliance on a combination of internal SOC resources and an outsourced external vendor for security operations, this playbook integrates the roles of both entities into a coordinated response. (CBC News, 2019) The utility wants to buy hardware and software to run a "security information event monitoring" tool for a security operations Centre that will be run by an outside vendor.

Scope:

This playbook covers ransomware-related incidents targeting NSP's IT and OT environments, both on-premises and cloud-based systems.

Assumptions:

- The external vendor (MSSP) has been pre-vetted and is familiar with NSP's IT infrastructure and security tools.
- Regular training and tabletop exercises are conducted for both internal and external teams.
- There is a functional, tested backup and disaster recovery (DR) plan in place for critical systems.

2. Incident Categorization

Criteria for Ransomware Incident Identification: Ransomware is a type of malware that locks you out of files or systems until you pay a ransom to a threat actor. Payment doesn't guarantee you will regain access to your information. (Canadian Centre for Cyber Security, n.d.).

An incident is categorized as ransomware if any of the following indicators are present:

- Encryption of files with a ransom note demanding payment in cryptocurrency.
- Network or system behavior that matches known ransomware tactics (e.g., network-wide file encryption, lateral movement).
- Detection by endpoint protection tools, SIEM, or network monitoring systems of suspicious or malicious activity that fits the ransomware profile.

---

3. Roles & Responsibilities: This section outlines the stakeholders involved in the incident response process and their specific duties. These can include incident response team members, IT staff, management, and external entities. (Cynet, n.d.)

In-House SOC:

- Incident Commander: Leads the response and makes high-level decisions.
- Threat Analysts: Work with the MSSP to analyze the ransomware variant and identify impacted systems.
- Incident Response Team: Coordinates across internal teams (IT, Legal, PR, etc.) to ensure a coordinated response.
- IT Infrastructure Team: Works to isolate and contain infected systems.
- Communication Team: Responsible for managing internal and external communications.

External Vendor (MSSP):

- Detection & Analysis: Provides expertise in analyzing ransomware strain, attack vectors, and identifying affected assets.
- Containment & Remediation: Helps implement containment strategies and assist in removing ransomware from affected systems.

- Incident Triage & Support: Provides additional resources for triage, containment, and recovery efforts during the incident.
- Expert Consultation: Offers specialized knowledge in threat intelligence, ransomware variants, and best practices for recovery.

Other Key Stakeholders:

- Legal Team: Provides guidance on legal and regulatory obligations (e.g., reporting to regulators, paying ransoms). Legal experts should review incident response plans, policies, and procedures to ensure their compliance with law and Federal guidance, including the right to privacy. (NIST, 2012)
- Public Relations (PR): Manages external communications and media interactions, particularly in case of public disclosure. Depending on the nature and impact of an incident, a need may exist to inform the media and, by extension, the public. (NIST, 2012)

4. Incident Response Phases

(a) Preparation

- Ensure a functional, regularly tested backup strategy. Implement a backup plan for your organization and backups should be done frequently to ensure your data is as close to real time as possible. (Canadian Centre for Cyber Security, n.d.).
- Define methods for handling classified information and data, if required. Establish communication channels (chat rooms, phone bridges) and a method for out-of-band coordination. Conduct regular ransomware-specific tabletop exercises. (CISA, 2024)
- Ensure endpoint protection, email filtering, and network security systems are in place and up to date.
- Establish an escalation matrix and pre-defined roles for incident response.

(b) Detection:

- Detection Tools: SIEM, EDR, IDS/IPS, and antivirus solutions should trigger alerts on suspicious activity (e.g., file encryption, ransom notes, unusual network traffic).
- MSSP Involvement: The external vendor will assist in confirming the nature of the incident and conduct initial analysis.

- Initial Triage: SOC and MSSP collaborate to identify the scope of the attack (which systems, departments, or business functions are impacted).

(c) Containment: Isolating impacted systems and network segments from each other and/or from non-impacted systems and networks. If this is needed, consider the mission or business needs and how to provide services so missions can continue during this phase to the extent possible. (CISA, 2024)

- Immediate Isolation: Disconnect affected systems from the network to prevent lateral movement of the ransomware. This includes workstations, servers, and network segments.
- MSSP Role: Assist in identifying compromised accounts, reviewing logs, and ensuring that infected systems are isolated promptly.
- Network Segmentation: Segment the network to prevent ransomware from spreading further (e.g., isolating OT from IT).

(d) Eradication

- Ransomware Removal: Remove ransomware and associated artifacts from infected systems. Remediating all infected IT environments (e.g., cloud, OT, hybrid, host, and network systems). (CISA, 2024)
- MSSP Support: External vendor assists in removing ransomware and providing insights into persistent threats.
- Restore from Backup: Restore clean backups to the affected systems after ensuring they are free from ransomware. Replacing compromised files with clean versions. (CISA, 2024)

(e) Recovery

- Restore Operations: Prioritize critical systems and services for restoration based on business impact. Once you are confident, restore your systems and devices from your secure backup. (Canadian Centre for Cyber Security, n.d.)
- System Integrity Check: Conduct thorough integrity checks on recovered systems to ensure they are free of malware.
- Communication: Inform stakeholders of recovery progress, including timelines for full system restoration.

- Monitor: Use endpoint protection and network monitoring tools to ensure no residual ransomware or malicious activity remains.

(f) Lessons Learned

- Post-Incident Review: Conduct a joint review between the internal SOC and the MSSP to assess the effectiveness of the response, identify areas of improvement, and adjust the playbook as necessary.
- Report Creation: Document the entire incident for regulatory and compliance purposes. Provide post-incident updates as required by law and policy. Work with CISA to provide the required artifacts, close the ticket, and/or take additional response action. (CISA, 2024)
- Preventative Measures: Update security policies, conduct additional training, and implement additional measures to prevent future incidents (e.g., multi-factor authentication, improved patch management). Improving tools required to perform protection, detection, analysis, or response actions. (CISA, 2024)

5. Communication Protocol

Internal Communication:

- Use encrypted, internal channels for communication during the incident.
- Keep management and all key departments (IT, PR, Legal, etc.) informed of progress at regular intervals.

External Communication:

- Law Enforcement: If applicable, engage with local or federal law enforcement (e.g., RCMP or the Canadian Cyber Incident Response Centre) to report the ransomware attack.
- Vendors: Work with external vendors, including IT service providers and backup storage vendors, to restore services.
- Customers & Partners: Be prepared with a pre-determined messaging strategy for external communications, focusing on customer impact and mitigation efforts.
- Regulatory Bodies: Report the incident to the Office of the Privacy Commissioner of Canada if personal data is compromised. Report the ransomware attack to loca

- law enforcement, the Canadian Anti-Fraud Centre and the Canadian Centre for Cyber Security. (Canadian Centre for Cyber Security, n.d.)

Policy Outline 1: Ransomware Detection and Response Policy

Purpose:

The purpose of this policy is to define how Nova Scotia Power (NSP) detects and responds to ransomware incidents, ensuring swift identification, containment, and resolution to minimize impact on critical systems and operations.

Importance:

- Reduced cost of attack: As with most IT-related security incidents, a well-planned and executed response can greatly reduce the impact and cost of a ransomware attack. (LORICCA, 2021)
- Operational Continuity: Effective response ensures that NSP's core services, including power generation and distribution, remain operational during and after an incident.
- Data Protection: Mitigates risks to sensitive customer and organizational data by containing and eradicating ransomware promptly.

Activities and Responsibilities:

- Monitoring: Utilize a combination of Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR) tools, and MSSP support for continuous monitoring of potential ransomware indicators.
- Detection: SOC and MSSP teams must collaborate to detect ransomware variants through alerts triggered by unusual activity, file encryption, or ransom notes. Implement an intrusion detection system (IDS) to detect command and control activity and other potentially malicious network activity that occurs prior to ransomware deployment. (LORICCA, 2021)
- Initial Response: Upon detection, the Incident Commander (SOC) must lead the team to isolate affected systems and activate the incident response playbook.
- Investigation: SOC and MSSP will investigate the attack, identify impacted systems, and escalate as necessary.

Playbook Reference: Section 2 - Detection, Section 3 - Roles & Responsibilities

Consequences of Non-Compliance:

- Delayed Detection: Late identification can lead to greater spread, extended downtime, and increased recovery costs.
- Operational Disruption: Failure to detect and respond appropriately may result in prolonged service outages, damaging NSP's reputation and customer trust.

Policy Outline 2: Ransomware Containment and Eradication Policy

Purpose:

This policy outlines the procedures and responsibilities for containing and eradicating ransomware threats within NSP's IT and OT environments to prevent further damage and secure operational systems.

Importance:

- Prevents Lateral Movement: Proper containment prevents ransomware from spreading across the network and affecting additional systems or departments.
- Critical Infrastructure Protection: Ensures that key infrastructure systems (such as power grid control systems) are protected from the effects of ransomware.
- Data Integrity and Recovery: Secures systems for effective recovery while ensuring that clean data is restored without reinfection.

Activities and Responsibilities:

- Containment: Immediate isolation of infected systems from the network to prevent further lateral movement. SOC and IT teams must isolate systems and services, such as OT or critical infrastructure, and ensure communications are not compromised. Once a system has been identified as having ransomware, the potentially infected computer should be quickly isolated from the network (including WIFI) to prevent further spread of the malware. (LORICCA, 2021)
- Ransomware Eradication: After containment, the SOC, with the assistance of MSSP, will work to remove all traces of ransomware, including backdoors and malware persistence mechanisms, from infected systems.
- System Integrity Checks: Prior to recovery, ensure that all infected systems are thoroughly scanned and cleaned of ransomware and any residual malware.

Playbook Reference: Section 4 - Containment & Eradication

Consequences of Non-Compliance:

- Further Spread: Failure to contain ransomware promptly can lead to a wider attack, affecting more systems, including critical infrastructure.
- Ineffective Recovery: Inadequate eradication of ransomware may result in reinfection during recovery, prolonging downtime and increasing the risk of data loss.
- Operational Downtime: Delays in containment and eradication may significantly impact NSP's ability to restore services and operations in a timely manner. Data breaches cause downtime, sinking productivity and profits. (Sprinto, n.d.)

Policy Outline 3: Ransomware Communication and Reporting Policy

Purpose:

This policy establishes the framework for internal and external communication during a ransomware incident, ensuring that stakeholders are informed, regulatory obligations are met, and the company's reputation is managed.

Importance:

- Transparency and Trust: Clear communication with employees, customers, regulators, and the public is essential to maintaining trust and managing reputational risk during a cyberattack.
- Regulatory Compliance: NSP must comply with relevant data breach and cybersecurity reporting requirements under Canadian law (e.g., PIPEDA) and industry best practices.
- Coordinated Effort: Proper communication ensures that all teams, including SOC, IT, Legal, PR, and external stakeholders, are aligned on the incident's scope, impact, and resolution efforts.

Activities and Responsibilities:

- **Internal Communication**: The SOC must keep internal stakeholders (management, IT, Legal, etc.) informed about the status of the incident, including its scope, impact, and resolution efforts.
- **External Communication**: The PR and Legal teams, under guidance from the Incident Commander, will handle all external communication, including customer notifications, media responses, and regulatory filings.

- **Regulatory Reporting**: The Legal team ensures that regulatory bodies, such as the Office of the Privacy Commissioner of Canada, are notified within the prescribed timeframes if personal data is involved.

Playbook Reference: Section 5 - Communication Protocol

Consequences of Non-Compliance:

- **Reputational Damage**: Poor or delayed communication could lead to loss of public trust and damage NSP's reputation, particularly with customers who may be affected. Non-compliance can quickly cause customers to lose trust and loyalty. People will look for alternative solutions and choose those that take security and compliance more seriously. (Sprinto, n.d.)
- **Legal and Regulatory Penalties**: Failing to meet regulatory reporting requirements could result in legal sanctions, fines, and compliance audits.
- **Misalignment of Efforts**: Without coordinated communication, different teams may work in silos, reducing the effectiveness of the incident response and recovery efforts.

Reference

Nova Scotia Power. (n.d.). *Privacy statement*. Nova Scotia Power. https://www.nspower.ca/privacy-statement

Canadian Centre for Cyber Security. (n.d.). *Developing your incident response plan (ITSAP.4000.3)*. Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/guidance/developing-your-incident-response-plan-itsap40003

Cynet. (n.d.). *Incident response plan template*. Cynet. https://www.cynet.com/incident-response/incident-response-plan-template/

National Institute of Standards and Technology. (2012). *Computer security incident handling guide (Special Publication 800-61 Revision 2)*. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Cybersecurity and Infrastructure Security Agency (CISA). (2024). *Federal government cybersecurity incident and vulnerability response playbooks* (Rev. 508C). U.S. Department of Homeland Security. https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

Canadian Centre for Cyber Security. (n.d.). *Ransomware: How to prevent and recover (ITSAP.0009.9)*. Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/guidance/ransomware-how-prevent-and-recover-itsap00099#recover

LORICCA. (2021). *Ransomware prevention and response policy* (Version 1). https://loricca.com/wp-content/uploads/2021/06/Ransomware-Prevention-and-Response-Policy-2021-1.pdf

Sprinto. (n.d.). *Consequences of non-compliance*. Sprinto. https://sprinto.com/blog/consequences-of-non-compliance/#:~:text=Ignoring%20security%20rules%20makes%20it,to%20complete%20loss%20of%20business.