**Incident Response Playbook for Nova Scotia Power  
Introduction**

Nova Scotia Power, a critical infrastructure provider in the energy sector, ensures the reliable generation, transmission, and distribution of electricity across Nova Scotia. Its operations involve complex systems, including IT networks and industrial control systems like SCADA. These systems are essential to providing uninterrupted power to businesses, homes, and critical services throughout the region.

Due to the nature of its services, Nova Scotia Power faces unique cybersecurity challenges. These include potential cyberattacks on operational technologies, ransomware threats, and data breaches that could compromise customer data and disrupt energy delivery. Regulatory compliance, such as adherence to NERC CIP standards, further emphasizes the importance of a robust incident response framework.

This playbook is designed to provide a clear, step-by-step approach to managing and mitigating security incidents. It integrates the NIST 4-step incident process, ensuring comprehensive coverage from preparation to recovery. The document will serve as a guide for Nova Scotia Power’s Cybersecurity Incident Response Team (CSIRT) and stakeholders to handle incidents effectively and maintain operational resilience.

**Incident Playbook Development**

**1. Company Information**

* **Company Name**: Nova Scotia Power\*
* **Contact Titles (Positions)**:
  + Chief Information Officer (CIO)\*
  + Chief Operations Officer (COO)\*
  + Compliance Manager\*
  + Incident Response Team (IRT) Lead\*
  + Customer Service Director!
* **Contact Availability**: 24/7 for CIO, COO, and IRT Lead; business hours for others!
* **Contact Data Permissions (TLP)**:
  + TLP: RED for internal teams.
  + TLP: AMBER for regulators.
  + TLP: GREEN for external partners.

**2. Incident Information**

* **Incident Name**: SCADA System Ransomware Attack!
* **Incident Type**: Cyberattack targeting operational technology (OT) infrastructure.
* **C Effect (Confidentiality Impact)**: Exposure of sensitive grid management data.
* **I Effect (Integrity Impact)**: Alteration of grid control settings, leading to potential outages.
* **A Effect (Availability Impact)**: Disruption of power supply to customers.

**3. Team Members (CSIRT)**

* Incident Response Manager\*
* Cybersecurity Analyst\*
* IT Operations Lead\*
* Legal Counsel!
* Public Relations Specialist!

**4. Internal Stakeholders**

* Executive Leadership Team\*
* IT and OT Teams\*
* Customer Support Teams!
* Compliance Department\*

**5. External Stakeholders**

* Nova Scotia Utility and Review Board (UARB)\*
* Federal Energy Regulatory Commission (FERC)\*
* Emergency Response Partners (local law enforcement, CERT)\*
* Affected Customers!
* Media Contacts!

**6. Incident Playbook Steps**

1. **Preparation**
   * Identify critical systems and assets (e.g., SCADA, servers).
   * Conduct regular training and simulations for the CSIRT.
   * Maintain updated contact lists for stakeholders.
2. **Detection and Analysis**
   * Monitor for unusual traffic patterns or ransomware indicators.
   * Utilize SIEM tools to analyze logs and alerts.\*
   * Isolate affected systems immediately upon detection!
3. **Containment, Eradication, and Recovery**
   * Short-Term Containment: Disable access to infected systems.
   * Eradication: Remove ransomware, restore from backups.
   * Recovery: Validate integrity of restored systems, resume operations.
4. **Post-Incident Activity**
   * Conduct a lessons-learned meeting.
   * Update the playbook based on findings.
   * Submit reports to UARB and other regulators.

**7. Key Escalation Triggers**

1. **SCADA System Affected**
   * Escalate to CIO and COO.
   * Reasoning: Ensures executive oversight for operational disruptions.
2. **Customer Data Breach**
   * Escalate to Legal Counsel and Privacy Officers.
   * Reasoning: Comply with PIPEDA notification requirements.
3. **Critical Infrastructure Downtime**
   * Escalate to UARB and FERC.
   * Reasoning: Regulatory compliance and risk management.
4. **Media Coverage of Incident**
   * Escalate to Public Relations Specialist.
   * Reasoning: Control public narrative and maintain trust.
5. **Financial Impact Exceeds Threshold**
   * Escalate to Board of Directors.
   * Reasoning: Address potential shareholder concerns.

**8. Stakeholder Notifications**

1. **Internal Teams**: Details of containment and recovery plans. Necessary for coordination and execution.
2. **Regulators**: Summary of incident, timeline of events, and remediation steps. Ensures compliance with legal obligations.
3. **Customers**: Clear, concise information on service impacts and timelines for resolution.
4. **Emergency Response Teams**: Detailed technical data for collaborative containment efforts.
5. **Media**: High-level summaries to maintain transparency while safeguarding sensitive details.

**Reflection and Data Analysis**

**Reflection**

The playbook development process highlighted the importance of:

* Detailed stakeholder mapping.
* Clear escalation triggers and communication protocols.
* Real-world data integration for accuracy and feasibility.

**Required Policies**

1. **Incident Detection Policy**
   * Rationale: Allows proactive monitoring and detection of anomalies.
2. **Data Classification Policy**
   * Rationale: Ensures consistent prioritization of assets and data.
3. **Incident Reporting Policy**
   * Rationale: Aligns with legal requirements for timely stakeholder notification.
4. **Access Control Policy**
   * Rationale: Limits exposure of critical systems to minimize risk.
5. **Incident Testing Policy**
   * Rationale: Validates the effectiveness of the playbook and CSIRT readiness.

**Incident Playbook Case Study Data Template**

|  |  |  |
| --- | --- | --- |
| **Data Name** | **Content** | **Rationale** |
| **Company Information** |  |  |
| Company Name | Nova Scotia Power\* | Company is critical infrastructure provider. |
| Contact Title (Position) | CIO, COO, Compliance Manager, IRT Lead, PR Specialist | Critical roles for incident response. |
| Contact Availability | 24/7 for CIO, COO, IRT Lead | Rapid decision-making and response coordination. |
| Contact Data Permissions (TLP) | TLP:RED, TLP:AMBER, TLP:GREEN | Aligns with information sensitivity and sharing needs. |
| **Incident Info** |  |  |
| Incident Name | SCADA System Ransomware Attack! | Incident targeting operational technology systems. |
| Incident Type | Ransomware | Specific threat impacting availability and integrity. |
| C Effect | Exposure of sensitive grid management data. | Confidentiality of critical data at risk. |
| I Effect | Alteration of grid control settings. | Potential to disrupt system integrity. |
| A Effect | Power supply disruption. | Direct impact on availability of services. |
| **Team Members (CSIRT)** |  |  |
| Roles | Incident Manager, Analyst, IT Lead, Legal Counsel | Core team for technical and legal resolution. |
| **Internal Stakeholders** |  |  |
| Executive Team | Leadership for strategy and decisions. |  |
| IT and OT Teams | System experts for containment and recovery. |  |
| Compliance Team | Ensures regulatory adherence. |  |
| **External Stakeholders** |  |  |
| UARB | Regulator for incident reporting. |  |
| FERC | Federal compliance entity. |  |
| Customers | Stakeholders affected by disruptions. |  |
| **Reports and Testing** |  |  |
| Reports Required | Incident summary, regulatory notifications | Accountability and compliance documentation. |
| Testing Frequency | Quarterly | Ensures readiness and relevance of playbook. |