Ransomware Incident Response Policies

Feb 18, 2025

Protecting BC Ferries' Operations and Customer Trust

Violet Figueroa

Why Ransomware Policies Matter

- Ransomware attacks can disrupt ferry operations, compromise customer data, and harm BC Ferries' reputation.
- Policies provide clear guidelines to prevent, detect, and respond to ransomware incidents.
- Consequences of non-compliance:
  - Financial losses from downtime or ransom payments.
  - Legal penalties under PIPEDA for mishandling customer data breaches.
  - Loss of public trust and customer confidence.

	TLP: RED	TLP: AMBER	TLP: GREEN	TLP: WHITE
Information sharing boundaries	**Not for disclosure** **Restricted to participants only**	**Limited disclosure** **Participant organisations only**	**Limited disclosure** **Restricted to community only**	**Disclosure is not limited**
When to use	Impacts privacy, reputation or operations	Risk to privacy, reputation or operations if shared outside participating organisations	Useful for participating organisations and broader community	Minimal or no foreseeable risk of misuse, suitable for public release
How to share	Participating organisations only	Organisation members only. Additional restrictions can be set.	Peer and partner organisations only. Not suitable for public release	No restrictions

What is a Ransomware Incident Response Plan?

- A structured approach to managing ransomware attacks.
- Key goals:
  - Minimize operational disruptions.
  - Protect sensitive data (e.g., customer PII).
  - Ensure compliance with regulatory requirements (e.g., PIPEDA, DFSR).

How We Handle Ransomware Incidents

1. Preparation
2. Detection & Analysis
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned (NIST SP 800-61 framework)

Why?

It ensures a systematic response to minimize impact on ferry operations.

Policies Supporting Ransomware Response

- Data Access Policy:
  - Restricts access to sensitive systems to authorized personnel only.
  - Prevents unauthorized changes to critical systems.
  - During the "Detection & Analysis" phase, the Data Access Policy ensures that access logs are available for review by Security Analysts to identify unauthorized access or suspicious activity.
  - During the "Containment" phase, access controls outlined in this policy prevent unauthorized personnel from accessing affected systems, reducing the risk of further compromise.
  - The policy supports post-incident analysis by ensuring all access is logged and monitored, aiding in forensic investigations.

Policies Supporting Ransomware Response

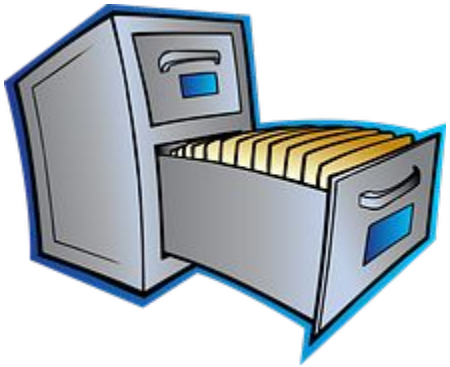
- Backup Policy:
  - Ensures regular backups of critical systems are stored securely offsite.
  - Facilitates recovery without paying ransom demands.
  - The Backup Creation, Storage, and Restoration Procedure ensures these policies are actionable during incidents.
  - During the "Recovery" phase, the Backup Policy ensures that clean backups are securely stored and available for restoring encrypted systems without paying ransom demands.
  - The policy aligns with the "Preparation" phase by requiring regular testing of backups to confirm their integrity and usability in case of an incident.
  - It supports the "Lessons Learned" phase by providing documentation of backup performance during recovery efforts.

Policies Supporting Ransomware Response

- Network Segmentation Policy:
  - Isolates IT systems from OT systems to prevent ransomware spread.
  - The Network Segmentation Procedure provides detailed steps for isolating IT and OT systems.
  - During the "Containment" phase, this policy ensures that IT and OT systems are isolated to prevent ransomware from spreading across network segments.
  - The policy supports the "Detection & Analysis" phase by enabling effective monitoring of traffic between network segments using Intrusion Detection Systems (IDS).
  - It facilitates rapid response during escalations by allowing infected segments to be quickly isolated without disrupting unaffected areas.

Policies Supporting Ransomware Response

- Data Retention and Destruction Policy:
  - Defines how long sensitive data is retained and ensures secure deletion when no longer needed.
  - The Log Retention Policy supports the Detection & Analysis phase of the playbook by ensuring logs are available for incident investigation.
  - During the "Detection & Analysis" phase, this policy ensures that retained data is available for forensic analysis while defining clear guidelines for preserving logs required for investigations.
    The policy supports the "Lessons Learned" phase by requiring secure destruction of unnecessary data after incidents, reducing future exposure risks.
  - It aligns with compliance requirements during the "Recovery" phase by ensuring sensitive data is handled according to regulatory standards.

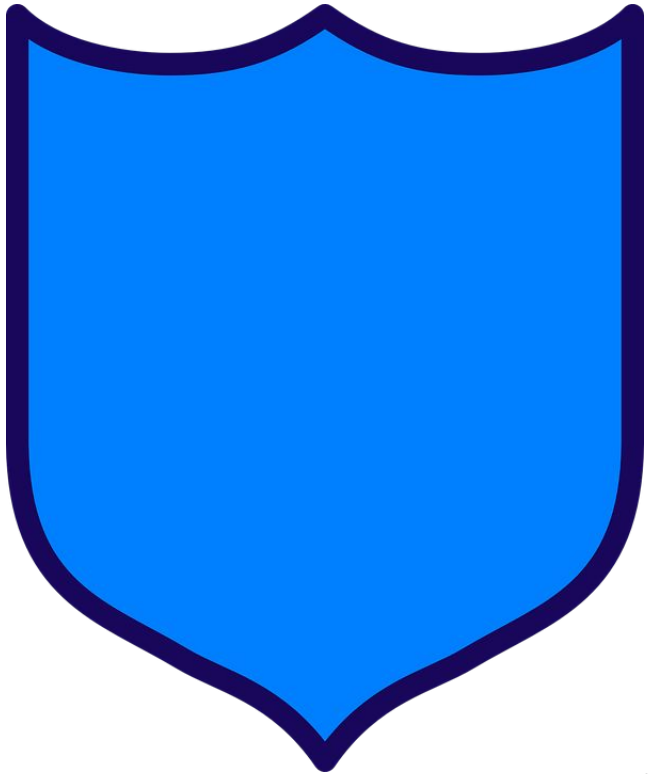


Policies Supporting Ransomware Response

- Log Retention Policy:
  - Preserves logs for incident analysis and regulatory reporting.
  - The Log Retention Policy supports the Detection & Analysis phase of the playbook by ensuring logs are available for incident investigation.
  - During the "Detection & Analysis" phase, this policy ensures that logs are retained and accessible for identifying Indicators of Compromise (IOCs) and analyzing ransomware activity.
  - The policy supports escalation triggers in the playbook by preserving logs required for regulatory reporting (e.g., PIPEDA breach notifications).
  - It aligns with the "Lessons Learned" phase by maintaining logs for post-incident reviews to improve future incident response processes.

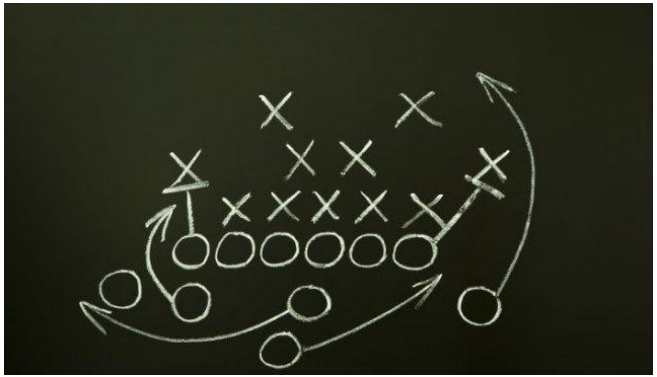
The Role of Policies in Preventing Damage

- Prevent unauthorized access to critical systems and sensitive data.
- Ensure compliance with PIPEDA
- Ensuring a Breach Notification within 72 hours
- Enable quick recovery by ensuring backups are available and secure.



How Playbooks Support Policies

- Playbook Steps for Ransomware Response:
  - Detect ransomware activity using network monitoring tools (e.g., SIEM).
  - Contain the attack by isolating affected systems from the network.
  - Restore encrypted systems from clean backups stored offsite.
  - Notify regulators (e.g., Transport Canada, PIPEDA) if required by law.



What Happens If We Don’t Follow Policies?

- For BC Ferries:
  Regulatory fines (e.g., PIPEDA violations for mishandling customer PII).
  - Operational disruptions leading to financial losses.
  - Reputational damage affecting customer trust.
- For Employees:
  - Disciplinary action for failing to follow security protocols.
  - Potential legal liability in cases of negligence.

Clear Communication During Incidents

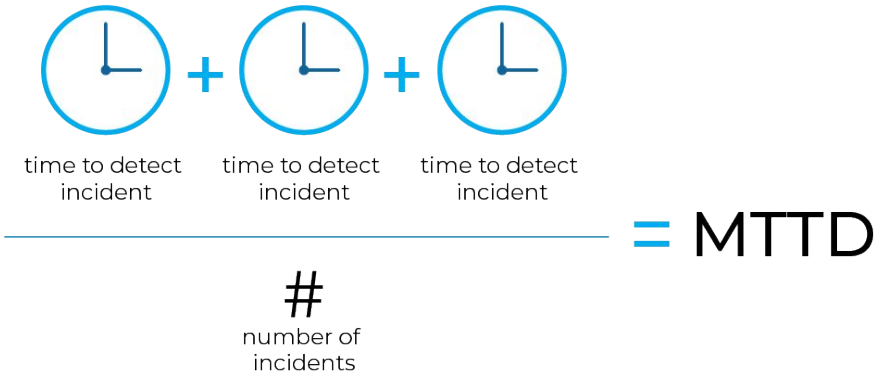
- Internal Communication:
  - Notify the Incident Response Team (IRT) immediately upon detection of ransomware activity.
    Provide regular updates to executive leadership on incident progress.
  - Safeguard credentials under the Data Access Policy.
  - Report suspicious activity as outlined in the Log Retention Policy.
- External Communication:
  - Notify customers if their data is compromised (PIPEDA requires notification within 72 hours).
  - Report operational disruptions caused by ransomware to Transport Canada under DFSR.

Restoring Operations Safely

- Steps to Recovery:
  - Secure the environment by removing ransomware from affected systems.
  - Restore encrypted systems using clean backups stored offsite.
  - Test restored systems before reconnecting them to production environments.
- Importance of timely recovery:
  - Reduces downtime costs and maintains customer trust.

How We Measure Effectiveness

- Key Metrics for Ransomware Response:
  - Mean Time to Detect (MTTD): Speed of identifying ransomware activity.
  - Mean Time to Respond (MTTR): Efficiency in containing and recovering from the attack.
  - Percentage of incidents resolved within SLA timelines.



Empowering Our Team Against Ransomware

- Regular training on recognizing phishing attempts and other ransomware entry methods.
- Simulations to test readiness (e.g., tabletop exercises simulating ransomware attacks).
- Consequences of inadequate training:
  - Increased vulnerability to attacks due to human error (e.g., clicking on phishing links).

Learning From Ransomware Incidents

- Conduct root cause analysis after every ransomware incident.
- Update policies, playbooks, and employee training based on lessons learned.
- Document findings to improve future responses.
- Review detailed procedures in your department's internal portal.
- Participate in upcoming training sessions on ransomware prevention.


Thank You For Your Time!

1. National Institute of Standards and Technology. (2012). *Computer Security Incident Handling Guide* (SP800–61 Rev.2). https://doi.org/10.6028/NIST.SP.800–61r2
2. Transport Canada. (2021). *Domestic Ferries Security Regulations*. https://tc.canada.ca/en/marine-security/domestic-ferries-security-regulations
3. Office of the Privacy Commissioner of Canada (PIPEDA). (2000). *Personal Information Protection and Electronic Documents Act*. https://www.priv.gc.ca/en/
4. Whitman, M., & Mattord, H. (2017). *Principles of information security* (6th ed.). CENGAGE Learning Custom Publishing.
5. Cybersecurity and Infrastructure Security Agency (CISA). (2021). *Incident and Vulnerability Response Playbooks*. Retrieved February 19, 2025, from https://www.cisa.gov/publication/cybersecurity-playbooks