Title: Ransomware Incident Response Playbook

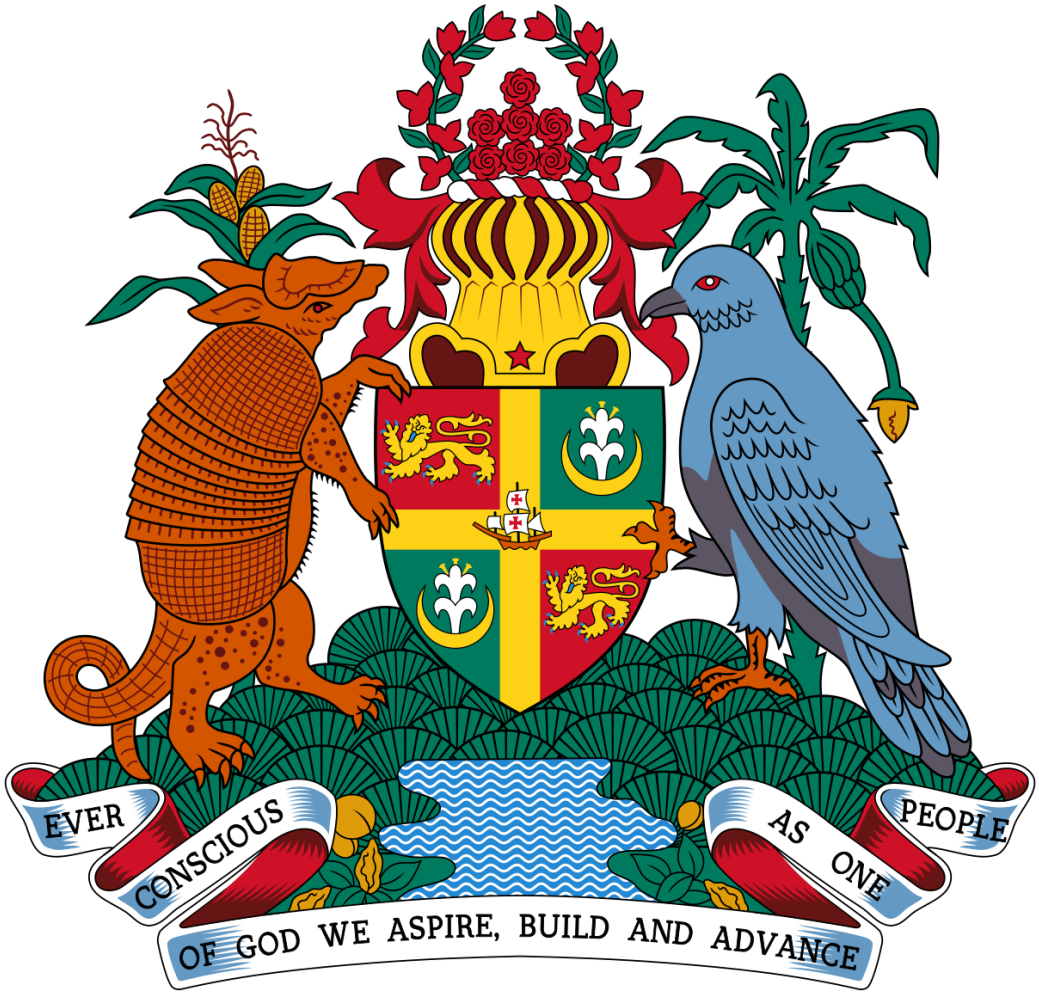
Subtitle: A Structured Response Framework for the Ministry of Education, Youth, Sports & Culture

Student Name: Ahndre Walters

Cohort: Cyber Nations Grenada – Cohort 1

Ministry Investigated: Ministry of Education, Youth, Sports & Culture

Submission Date: May 9, 2025



Declaration: I certify that this submission is my original work and complies with the guidelines for this assignment.

TABLE OF CONTENTS

INTRODUCTION

A ransomware playbook is a structured document outlining the step-by-step actions an organisation should take during a ransomware attack. It ensures that incident responders act swiftly, consistently, and effectively to minimize damage and restore systems securely.

In the public sector, ransomware can disrupt critical services, compromise sensitive citizen data, and erode public trust. In this scenario, the breach was initiated through a cleverly disguised USB drop using social engineering. The ransomware exploited outdated protections and inadequate segmentation, spreading laterally before encrypting systems and demanding a $1 million ransom.

This playbook provides the Ministry of Education, Youth, Sports & Culture with a repeatable and adaptable framework for responding to ransomware attacks. It supports both technical responders and leadership teams in coordinating an effective and timely response.

RANSOMWARE INCIDENT RESPONSE STEPS

Triage

Objective: Identify and classify the threat quickly to initiate the appropriate response.

Actions:

- Log the time and source of the initial report, such as the receptionist's workstation at the time of detection.
- Notify the cybersecurity incident response team (CSIRT).
- Disconnect the affected system from the network.
- Confirm signs of encryption, ransom notes, or lateral movement.
- Check for ongoing infection or spread to other systems.
- Categorize severity as "High" due to government-wide encryption and data exfiltration.
- Begin documentation and preserve volatile evidence (RAM, processes, active sessions).

Investigation

Objective: Understand the scope, origin, and mechanics of the attack.

Actions:

- Retrieve and analyse the malicious USB and file (e.g. Invoice_Request.pdf) forensic evidence.
- Review endpoint logs, SIEM events, USB connection logs, and firewall activity.
- Identify infection vector through social engineering and USB delivery.
- Trace lateral movement paths through shared drives and unsegmented VLANs.
- Identify command-and-control (C2) communication attempts.
- Work with forensic analysts to map affected systems and detect exfiltrated data.

Containment

Objective: Stop the ransomware from spreading further.

Actions:

- Isolate infected devices including receptionist PC, ministry servers, and affected departments.
- Disable all USB ports organisation wide.
- Revoke compromised accounts or admin privileges.
- Block known malicious IPs/domains in the firewall.
- Disable vulnerable services such as Windows SMB or shared file servers to limit ransomware spread.
- Inform all users not to connect any devices or open suspicious files.

Eradication

Objective: Remove all traces of the ransomware and vulnerabilities.

Actions:

- Run antivirus and EDR scans across all endpoints.
- Use system backups to compare file integrity and detect persistence mechanisms.
- Patch vulnerable systems such as Windows SMB and endpoint security clients.
- Reinstall operating systems where necessary.
- Disable accounts with anomalous behaviour and change passwords ministry-wide.

Recovery

Objective: Restore normal services safely and confidently.

Actions:

- Restore data from clean, offline backups to ensure integrity and avoid reinfection.
- Gradually reconnect systems to a segmented and monitored network.
- Monitor systems for anomalies or C2 beaconing.
- Test functionality of all services (mail, DNS, internal databases).
- Communicate progress updates to internal and external stakeholders.

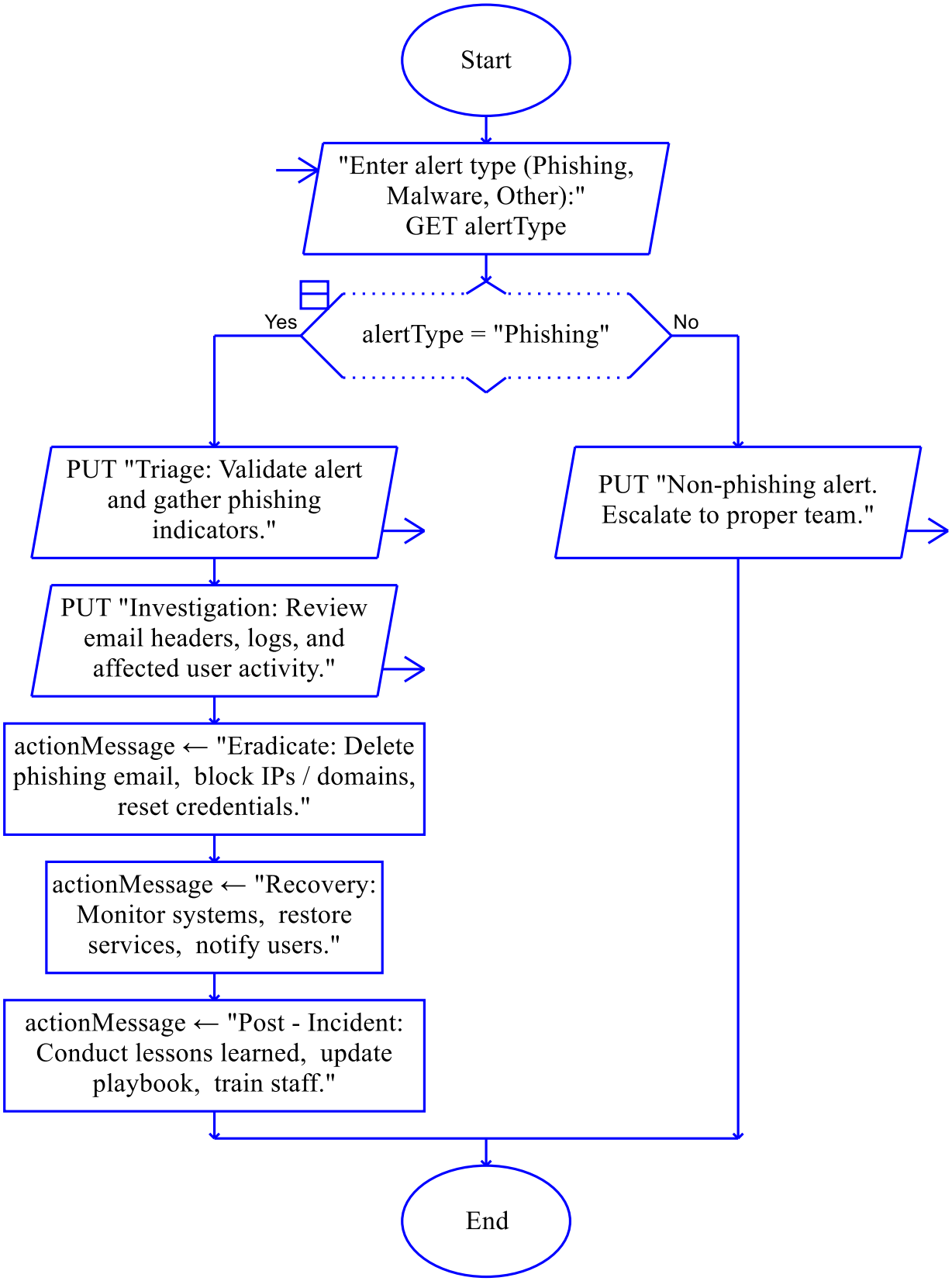
Post-Incident Activities

Objective: Strengthen defences and institutional knowledge.

Actions:

- Conduct a formal post-incident review with all involved teams.
- Document incident timeline, vulnerabilities, and response outcomes.
- Revise cybersecurity policies by disabling USB access and strengthening endpoint protection.
- Resume postponed security training initiatives.
- Report the breach to national cybersecurity authorities and affected individuals.
- Update and test this playbook with tabletop exercises.

FLOWCHART DIAGRAM



TOOLS, TEAMS & CONTROLS

Security Tools:

1. Endpoint Detection & Response (EDR) - to detect and isolate infected hosts.
2. Backup & Recovery Solutions - to restore clean system images.
3. SIEM tools (Splunk, Azure Sentinel) – used to correlate logs and detect abnormal patterns across systems.
4. USB Port Control Software - to block unauthorized device usage.
5. Network Segmentation & VLAN Configuration - to contain lateral spread.

Response Team:

- IT Security Team – Handles scanning, patching, isolation, and technical recovery.
- Incident Response Team (IRT) – Oversees coordination, prioritization, and escalation of the response.
- Legal & Compliance: Handling regulatory disclosure and liability assessment.
- Communications/Public Relations: Managing press releases and citizen notices.

LESSONS LEARNED & PREVENTION

- **Lesson 1**: Social engineering via physical delivery remains a potent threat.
- **Action**: Train frontline staff like receptionists on suspicious behaviours and reporting procedures.

- **Lesson 2**: USB security policies were ignored for convenience.
- **Action**: Enforce USB-blocking tools and use encrypted, organisation-issued drives only.

- **Lesson 3**: Poor network segmentation accelerated the spread.
- **Action**: Use VLANs and firewalls to segment departments such as Admin, IT, Guest, and Core Servers for improved isolation and control.

- **Lesson 4**: Delayed cybersecurity training weakened employee awareness.
- **Action**: Reinstate and mandate quarterly security awareness programs for all staff.

- **Lesson 5**: Outdated endpoint protection left systems vulnerable.
- **Action**: Automate AV updates and monitor for EDR agent failures.

- **Lesson 6**: Visitor access controls were halted.
- **Action**: Reintroduce visitor logs, badge policies, and supervised access.

CONCLUSION

This ransomware incident response playbook empowers the Ministry of Education, Youth, Sports & Culture with a clear, actionable framework to manage and recover from cyber threats swiftly and effectively. By aligning technical procedures with communication, compliance, and long-term resilience strategies, the Ministry strengthens its ability to safeguard critical data, protect public trust, and maintain operational continuity in the face of evolving ransomware attacks.