Incident Response Playbook

For

Cargojet Airways Limited

Prepared by

Jamiu Ayinde

Table of Contents

1. **Executive Summary**
2. **Roles, Responsibilities & Contact Information**
    - CEO
    - Cybersecurity Vendor
    - Incident Response Lead
    - Incident Response Team Members
3. **Incident Type: Malware Attack on Cargojet's Critical Systems**
    - Systems Affected
    - Threat Actor
    - Attack Vector
    - Detection Timeline
4. **Incident Response Process**
    - Step 1: Preparation
    - Step 2: Identification
    - Step 3: Containment
    - Step 4: Eradication
    - Step 5: Recovery
    - Step 6: Lessons Learned
    - Step 7: Communications
5. **Escalation Points and Justifications**
6. **Stakeholder Communication**
    - Internal Stakeholders
    - External Stakeholders
    - Sensitive Information to Withhold
7. **References**

Executive Summary

To safeguard the operational integrity and data confidentiality at Cargojet Airways Limited, we have developed this IRP to guide the Incident Response Team (IRT) through detecting, containing, eradicating, and learning from cybersecurity incidents. Partnering with CYBERDB for third-party incident response support, Cargojet's IRP aims to prevent data loss, service interruption, and reputational impact.

1. Roles, Responsibilities & Contact Information

Role	Responsibility	Contact Information
CSO / CISO	**Strategic lead. Develops technical, operational, and financial risk ranking criteria used to prioritize incident response plan.** **Authorizes when and how incident details are reported.** **Main point of contact for executive team and Board of Directors.**	**Name: Akeem** **Email: ak@cargojet.com**
Incident Response Team Lead and **Team Members**	**Central team that authorizes and coordinates incident response across multiple teams and functions through all stages of a cyber incident.** **Maintains incident response plan, documentation, and catalog of incidents.**	**Name: Kevin Incuben** **Email: Kincuben@cargojet.com**

	Responsible for identifying, confirming, and evaluating extent of incidents. **Conducts random security checks to ensure readiness to respond to a cyberattack.**	
Identity and Access Team Lead and Team Members	**Responsible for privilege management, enterprise password protection and role-based access control.** **Discovers, audits, and reports on all privilege usage.** **Conducts random checks to audit privileged accounts, validate whether they are required, and re-authenticate those that are.** **Monitors privileged account uses and proactively checks for indicators of compromise, such as excessive logins, or other unusual behavior.** **Informs incident response team of potential attacks that compromise privileged accounts, validates and reports on the extent of attacks.** **Takes action to prevent the spread of a breach**	**Name: Wale Adeniji** **Email: Wadenji@cargojet.com**

	by updating privileges.	
IT Operations and Support (internal)	**Manages access to systems and applications for internal staff and partners.** **Centrally manages patches, hardware and software updates, and other system upgrades to prevent and contain a cyberattack.**	**Name: Lanre Ifanyi** **Email:lanre@cargojet.com**
Legal Counsel	**Confirms requirements for informing employees, customers, and the public about cyber breaches.** **Responsible for checking in with local law enforcement.** **Ensures IT team has legal authority for privilege account monitoring.**	**Name: Akeem Ayinde** **Email: ak@cargojet.com**
Audit & Compliance	**Communicates with regulatory bodies, following mandated reporting requirements.**	**Name: Jide Olopoona** **Email: Jide@cargojet.com**
Human Resources	**Coordinates internal employee communications regarding breaches of personal information and responds to questions from employees.**	**Name: Ogundipe Lanrewal** **Email: Olanre@cargojet.com**
Marketing & Public Relations Lead	**Communicates externally with customers, partners,**	**Name: Micheal Chibuzo** **Email:**

	and the media. **Coordinates all communications and request for interviews with internal subject matter experts and security team.** **Maintains draft crisis communications plans and statements which can be customized and distributed quickly in case of a breach.**	**Micheal@cargojet.com**
Technical Support Lead (External)	**Provides security bulletins and technical guidance to external users in case of a breach.**	**Name: Jane Smit** **Phone** **Email: jane@cyberdb.com**

2. Incident Type: Malware Attack on Cargojet's Critical Systems

- **Systems Affected**: Flight scheduling servers *
- **Threat Actor**: Possible nation-state or organized criminal group *
- **Attack Vector**: Phishing link and malware installation *
- **Detection Timeline**: 2 hours *

3. Incident Response Process

- **Step 1: Preparation**
  - Regular training and policy review.
  - Maintain contact lists and ensure regulatory compliance.
- **Step 2: Identification**
  - Monitor servers and logs.
  - Immediate escalation if critical systems are compromised.
- **Step 3: Containment**
  - Isolate affected systems and engage CYBERDB if containment fails.

- **Step 4: Eradication**
    - Malware removal and system audit.
    - Escalate to CYBERDB if reinfection is detected.
- **Step 5: Recovery**
    - Restore systems and validate patching.
    - Escalate to Incident Response Lead if vulnerabilities persist.
- **Step 6: Lessons Learned**
    - Conduct a review and documentation.
    - Escalate procedural improvements to upper management.
- **Step 7: Communications**
    - Notify internal and external stakeholders with appropriate details.
    - Follow compliance and regulatory reporting standards.

5. Escalation Points and Justifications

Systems Affected: Cargojet's operational servers require priority escalation as they are mission-critical to daily operations.

Attack Confirmation: Upon identifying a phishing attempt with malware, escalate to the CSIRT Lead to initiate full containment.

Containment Failure: If containment measures fail, escalate to the identity and access management teams.

Detected Re-infection: Immediate escalation to CYBERDB for advanced forensic investigation and re-evaluation.

Post-Incident Gaps: Escalate findings from the lessons-learned phase to upper management to secure budget or resource adjustments for preventive measures.

6. Stakeholder Communication

- **Internal Stakeholders**: Executive Team, IT, Employees
- **External Stakeholders**: Customers, Regulatory Bodies
- **Sensitive Information to Withhold**: Attack specifics and system vulnerabilities.

Document Name	**Security Incident Response Plan**
Current Version	**Version 2**
Plan Owner	**Jamiu Ayinde**
Plan Approval	**Pauline Dhillon**
Date of Last Review	**October, 2024**

Cargojet Policy

https://docs.google.com/document/d/1GBF5b_ecLq_-71IJIqXAxOHMt2dEN6yo9kJRI0Jyjql/edit?usp=sharing

Power point Presentation

https://docs.google.com/presentation/d/1QDRSM1tUdxO5tcMj-liG1tzCHshJ5T4VjAbbccYU0kk/edit?usp=sharing

References

1. SANS Institute. (2023). *Incident Response Process: Best Practices for Effective Incident Management*. Retrieved from SANS Website
2. NIST. (2022). *Computer Security Incident Handling Guide* (SP 800-61r2). Retrieved from NIST Publications
3. PCI Security Standards Council. (2023). *PCI DSS Incident Response Guidelines*. Retrieved from PCI DSS
4. U.S. Department of Health and Human Services. (2023). *HIPAA Breach Notification Rule*. Retrieved from HHS HIPAA
5. European Union. (2022). *General Data Protection Regulation (GDPR)*. Retrieved from EU GDPR
6. National Institute of Standards and Technology. (2021). *Framework for Improving Critical Infrastructure Cybersecurity*. Retrieved from NIST Cybersecurity Framework
7. ISO/IEC. (2023). *ISO/IEC 27035: Information Security Incident Management*. Retrieved from ISO Standards
8. Cynet Security. (2022). *Incident Response Planning Template*. Retrieved from Cynet