Curtis Crawford

Lighthouse Labs

This playbook covers what to do in certain circumstances, the rules you need to follow (so that things go smoothly) and the least painful way to do it.

Incident Response (IR) Playbook

Table of Contents

Introduction1

Incident Response Team (IRT) 2

Incident Categorization and Prioritization 3

Incident Handling Procedures **4**

Communication Plan 5

Appendices 6

Supporting Policies7

References8

Introduction

**Purpose:**

To offer a systematic method for detecting, containing and neutralising cybersecurity incidents to minimise impact and support a speedy recovery.

**Scope:**

It is a playbook of rules for everyone who uses Cats’ Company’s information technology systems or handles its data, whether as an employee, contractor or third-party user.

**Audience:**

All IT staff, security personnel, and relevant stakeholders involved in incident response activities.

Incident Response Team (IRT)

**Roles and Responsibilities:**

**Incident Manager:**

Coordinates the incident response process.

Communicates with senior management.

**Technical Lead:**

Provides technical expertise.

Directs containment, eradication, and recovery efforts.

**Communication Lead:**

Manages internal and external communications.

Handles media inquiries and public statements.

**Legal Advisor:**

Ensures compliance with legal and regulatory requirements.

Advises on potential legal implications.

**IT Support:**

Assists with system recovery and technical issues.

Implements fixes and patches.

Incident Categorization and Prioritization

**Incident Types:**

Data Breaches

Malware Infections

Denial of Service Attacks

Unauthorized Access

**Severity Levels:**

**Low:** Minimal impact, routine handling.

**Medium:** Noticeable impact, requires immediate attention.

**High:** Significant impact, requires urgent response.

**Critical:** Severe impact, immediate and comprehensive response needed.

**Initial Triage Process:**

Assess the nature and scope of the incident.

Determine the severity level.

Assign the incident to the appropriate team members.

Incident Handling Procedures

**Preparation**

Conduct regular training and awareness programs.

Maintain an updated inventory of tools and resources.

**Identification**

Use monitoring tools to detect anomalies.

Implement a robust reporting mechanism for employees to report incidents.

**Containment**

Short-term Containment:

Isolate affected systems to prevent further damage.

**Long-term Containment:**

Implement temporary fixes while working on a permanent solution.

Eradication

Perform root cause analysis to identify the source of the incident.

Remove all traces of the threat from affected systems.

**Recovery**

Restore systems to normal operation.

Validate systems to ensure they are free from threats.

**Lessons Learned**

Conduct a post-incident review to identify improvements.

Update policies and procedures based on lessons learned.

Communication Plan

**Internal Communication:**

Regular updates to stakeholders.

Clear instructions for employees.

**External Communication:**

Notify affected parties (customers, partners).

Coordinate with law enforcement if necessary.

**Public Relations:**

Prepare public statements.

Manage media inquiries.

Appendices

**Glossary of Terms**

An “incident”:

an event that could result in loss of data, denial of service or a reputational loss for the company.

PII:

Personally Identifiable Information.

CVSS:

Common Vulnerability Scoring System.

Supporting Policies

**Data Retention and Destruction**

Policy: Set retention periods depending on data type and follow secure methods of destruction for obsolete data.

Procedure:

Identify data categories and assign retention periods.

Regularly audit data storage to ensure compliance.

Use approved methods to securely destroy data that is no longer needed.

**Log Management**

Policy: Log all critical systems and protect them properly, but check them regularly.

Procedure:

Configure logging on critical systems.

Review logs daily for suspicious activity.

Store logs securely and ensure they are tamper-proof.

**PII Handling**

Policy: Implement strict controls for accessing and sharing PII.

Procedure:

Limit access to PII to authorized personnel only.

Encrypt PII both in transit and at rest.

Regularly review access controls and update as needed.

**Incident Reporting**

Policy: Establish a clear incident reporting process.

Procedure:

Create a reporting mechanism for employees to report incidents.

Document all reported incidents.

Conduct regular training on the importance of incident reporting.

**Regulatory Compliance**

Policy: Ensure compliance with relevant laws and regulations.

Procedure:

Regularly review and update compliance policies.

Conduct periodic audits to ensure adherence to regulations.

Provide training on regulatory requirements.

References

* Cat’s Company’s Holes Revealed. (2023, July 24). Curtis Crawford, Lighthouse Labs.
* (Compass | IR Plan, Playbook, and Policy). (n.d.).
* NIST Special Publication 800-61 Revision 2. (2012). Computer Security Incident Handling Guide. National Institute of Standards and Technology. Retrieved from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>
* OWASP Foundation. (n.d.). OWASP Top Ten. Retrieved from <https://owasp.org/www-project-top-ten/>
* SANS Institute. (2018). Incident Handler's Handbook. Retrieved from <https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>
* International Organization for Standardization. (2013). ISO/IEC 27035:2013 - Information technology — Security techniques — Information security incident management. Retrieved from <https://www.iso.org/standard/44379.html>
* ChatGPT (2024) – Assisted with proper formatting – <https://www.ChatGPT.com>
* Information Systems Audit and Control Association (ISACA). (2012). Responding to Security Incidents. Retrieved from <https://www.isaca.org/resources/isaca-journal/issues/2012/volume-3/responding-to-security-incidents>
* Cisco Systems, Inc. (2015). Incident Response: Planning, Management, and Operations. Retrieved from <https://www.cisco.com/c/en/us/products/collateral/services/high-availability/white_paper_c11-732366.html>
* Center for Internet Security. (2019). CIS Controls: A Guide for Ensuring Security in Cyberspace. Retrieved from <https://www.cisecurity.org/controls/>
* Grammarly (2024) – Assisted with proper spelling and sentence structure – <https://www.grammarly.com>