Title: Incident Response Playbook

Version: 1.0  
Date: 29-10-2023  
Prepared by: Chris Chukwuma

Table of contents

1. Introduction
2. Purpose
3. Scope
4. Incident Response Policy
5. Incident Response Team
6. Incident Response Procedures
7. Incident Classification
8. Incident Reporting
9. Incident Assessment

10. Incident Containment

11. Incident Eradication

12.Incident Recovery

13.Post-Incident Analysis

14.Training and Awareness

15.Review and Maintenance

16. Appendices

**1. Introduction**  
The digital realm is fraught with risks, and the Incident Response Playbook is our shield against the onslaught of security threats. As cyber-attacks grow in sophistication, the need for a robust and agile response becomes paramount. This playbook is designed to be the cornerstone of our defense, providing the Incident Response Team (IRT) with the knowledge and procedures to tackle any security incident with confidence and efficiency.

In an era where data breaches can mean the downfall of a company, the IRT’s role is not just operational but strategic. The introduction of this playbook serves as a testament to our commitment to cybersecurity. It is a living document, evolving with the threat landscape, ensuring that our response is always one step ahead of potential attackers.

**2. Purpose**  
The purpose of this playbook is twofold: to minimize the impact of security incidents and to ensure a swift return to normal operations. By establishing a structured approach, we aim to mitigate risks, preserve customer trust, and maintain the integrity of our systems. This playbook is not just a set of instructions; it is a strategic asset that aligns with our broader security policies and business objectives.

A well-executed incident response can be the difference between a minor disruption and a major crisis. This playbook empowers our IRT to act decisively and effectively, ensuring that every member knows their role and the actions required of them. It is a blueprint for resilience in the face of cyber adversity.

**3. Scope**  
The scope of this playbook encompasses all IT systems, employees, and contractors within our organization. It is applicable to any security incident, whether it originates internally or externally, and covers a wide array of scenarios from data leaks to system breaches. The procedures herein are mandatory for all staff, ensuring a unified and effective response across the company.

This playbook also extends to our partners and vendors, as security is a shared responsibility. It outlines how external entities should coordinate with our IRT and adhere to our incident response protocols. By setting clear expectations, we create a cohesive defense against threats to our collective security.

**4. Incident Response Policy**

Our Incident Response Policy is a testament to our organization’s governance framework. It ensures that incident response activities align with corporate governance principles, providing clear directives for managing security incidents. This commitment to risk management establishes protocols that minimize the impact of incidents on business operations and compliance obligations.

In this policy, we emphasize regulatory compliance. We align with the NIST Cybersecurity Framework (CSF) version 2.0, adhere to GDPR requirements for data protection, strictly follow HIPAA/HITRUST standards for healthcare data, and maintain PCI/DSS compliance for payment processing. Senior management oversees our incident response capabilities, ensuring accountability and continuous improvement.

By integrating these elements, we enhance our incident response readiness and protect our organization against emerging threats.

**5. Incident Response Team**  
Our Incident Response Team is structured to uphold the principles of effective governance. Each member’s role is defined not just by their immediate tasks but also by their part in the broader risk management strategy. Members of the Incidence response team might include:

1. **Incident Manager**:
   * **Primary Responsibility**: The incident manager has overall responsibility and authority during an incident. They coordinate and direct all facets of the incident response effort.
   * **Secondary Responsibilities**: Everything that someone else isn’t assigned to. They may also devise and delegate ad hoc roles as required by the incident.
   * **Also Known As**: Chief Technical Officer, Information security officer.
2. **Tech Lead**:
   * **Primary Responsibility**: The tech lead is typically a senior technical responder. They develop theories about what’s broken, decide on changes, and run the technical team during the incident.
   * **Secondary Responsibilities**: Communicate updates to the incident manager and other team members, document key theories and actions taken during the incident, participate in incident postmortems, and page additional responders and subject matter experts.
   * **Also Known As**: Information security officer, SOC analyst.
3. **Communications Manager**:
   * **Primary Responsibility**: The communications manager is familiar with public communications, often from customer support or public relations teams. They write and send internal and external communications about the incident (including updates to the status page).
   * **Secondary Responsibilities**: Collect customer responses, interface with executives, and engage with other high-level stakeholders.
   * **Also Known As**: Communications officer, communications lead.
4. **Customer Support Lead**:
   * **Primary Responsibility**: Ensuring that incoming tickets, phone calls, and tweets related to the incident receive timely and appropriate responses.
   * **Secondary Responsibilities**: Passing customer-sourced details to the incident-response team.
   * **Also Known As**: Customer support coordinator.

Compliance is also a key consideration for the team. We will describe how the team’s actions adhere to internal policies and external regulations, ensuring that all response activities are conducted within the bounds of legal and ethical standards.

**6. Incident Response Procedures**

The Incident Response Procedures are the operational manifestation of our risk management framework. They provide a systematic approach to identifying, assessing, and responding to incidents, minimizing risks to information assets and business continuity. This section will be expanded to include detailed workflows that integrate risk assessment at every stage, ensuring that responses are proportionate to the severity of the incident.

We will also discuss the role of these procedures in maintaining compliance with industry best practices and regulatory requirements, emphasizing the importance of documentation and evidence preservation for potential legal scrutiny.

**Example Scenarios and Response Actions**

1. Open Cyber Attack

- Scenario: An unauthorized entity attempts to breach the company's firewall.

- Response Actions:

1. SOC Analyst identifies the breach attempt through monitoring systems.

2. Immediate firewall rule adjustments to block the attacking IP.

3. Conduct a thorough investigation to assess the extent of the breach.

4. Implement additional security measures.

5. Document the incident.

- Time Frame for Action: Immediate response within 30 minutes.

- Owner: SOC Analyst

- Risk Reports to: CTO

2. Privacy Incident

- Scenario: Unauthorized access to personal customer information.

- Response Actions:

1. SOC Analyst detects unusual access patterns.

2. Immediate revocation of compromised credentials.

3. Notification of affected customers and regulatory bodies.

4. Conduct a forensic analysis to understand the breach's origin.

5. Enhance security measures around personal data.

6. Document the incident.

- Time Frame for Action: Notification within 24 hours.

- Owner: ISO

- Risk Reports to: CTO

3. Data Leak

- Scenario: Confidential data is found on a public server.

- Response Actions:

1. SOC Analyst identifies and verifies the leak.

2. Remove the leaked data from public access.

3. Analyze how the data was exposed.

4. Notify affected parties and regulatory bodies.

5. Implement measures to prevent future leaks.

6. Document the incident.

- Time Frame for Action: Leak removal within 1 hour.

- Owner: SOC Analyst

- Risk Reports to: CTO

4. Denial of Service Attack

- Scenario: A website becomes unresponsive due to a flood of requests.

- Response Actions:

1. SOC Analyst detects unusual traffic spikes.

2. Deploy mitigation strategies such as rate limiting or IP blacklisting.

3. Redirect traffic to backup servers if necessary.

4. Conduct a post-attack analysis.

5. Strengthen DDoS protection measures.

6. Document the incident.

- Time Frame for Action: Mitigation within 15 minutes.

- Owner: SOC Analyst

- Risk Reports to: CTO

5. Service Alert

- Scenario: Monitoring systems detect abnormal activity in a critical service.

- Response Actions:

1. SOC Analyst investigates the alert.

2. If a threat is confirmed, isolate affected systems.

3. Perform a detailed threat assessment.

4. Restore services with enhanced security measures.

5. Document the incident.

- Time Frame for Action: Investigation within 1 hour.

- Owner: SOC Analyst

- Risk Reports to: CTO

6. Phishing Attack

- Scenario: Employees receive a phishing email attempting to steal credentials.

- Response Actions:

1. SOC Analyst identifies and blocks the phishing email.

2. Alert all employees about the phishing attempt.

3. Conduct a company-wide email security training session.

4. Review and enhance email security protocols.

5. Document the incident.

- Time Frame for Action: Employee notification within 1 hour.

- Owner: SOC Analyst

- Risk Reports to: CTO

7. Ransomware Attack

- Scenario: Systems are locked by ransomware demanding payment.

- Response Actions:

1. SOC Analyst detects the ransomware and isolates affected systems.

2. Inform law enforcement agencies.

3. Assess the impact and decide on the recovery approach.

4. Restore systems from backups.

5. Enhance anti-ransomware measures.

6. Document the incident.

- Time Frame for Action: Isolation within 30 minutes.

- Owner: ISO

- Risk Reports to: CTO

8. Insider Threat

- Scenario: An employee is detected exfiltrating sensitive data.

- Response Actions:

1. SOC Analyst detects suspicious activity.

2. Revoke the employee's access immediately.

3. Conduct a detailed investigation.

4. Take appropriate disciplinary action.

5. Strengthen monitoring of employee activities.

6. Document the incident.

- Time Frame for Action: Access revocation within 10 minutes.

- Owner: ISO

- Risk Reports to: CTO

**9. Malware Infection**

- Scenario: A system is compromised by malware.

- Response Actions:

1. SOC Analyst identifies and isolates the infected system.

2. Perform a full malware scan and removal process.

3. Investigate the source of the malware.

4. Update antivirus and anti-malware tools.

5. Document the incident.

- Time Frame for Action: Isolation within 15 minutes.

- Owner: SOC Analyst

- Risk Reports to: CTO

10. Network Intrusion

- Scenario: Unauthorized access to the internal network.

- Response Actions:

1. SOC Analyst detects and blocks the intrusion.

2. Conduct a thorough network sweep.

3. Assess the damage and identify vulnerabilities exploited.

4. Implement stronger network security measures.

5. Document the incident.

- Time Frame for Action: Blockage within 30 minutes.

- Owner: SOC Analyst

- Risk Reports to: CTO

11. SQL Injection Attack

- Scenario: An attacker uses SQL injection to access the database.

- Response Actions:

1. SOC Analyst detects abnormal database queries.

2. Block the offending IP address.

3. Audit and secure the database.

4. Patch the vulnerability in the application code.

5. Document the incident.

- Time Frame for Action: Blocking within 30 minutes.

- Owner: SOC Analyst

- Risk Reports to: CTO

12. Zero-Day Exploit

- Scenario: A system is compromised using a previously unknown vulnerability.

- Response Actions:

1. SOC Analyst detects the exploit activity.

2. Isolate affected systems.

3. Apply temporary fixes or workarounds.

4. Collaborate with vendors for a permanent patch.

5. Document the incident.

- Time Frame for Action: Isolation within 1 hour.

- Owner: ISO

- Risk Reports to: CTO

13. Social Engineering Attack

- Scenario: An attacker tricks an employee into divulging confidential information.

- Response Actions:

1. SOC Analyst identifies the breach.

2. Inform the targeted employee and change compromised credentials.

3. Conduct security awareness training.

4. Implement stricter verification protocols.

5. Document the incident.

- Time Frame for Action: Notification within 1 hour.

- Owner: ISO

- Risk Reports to: CTO

14. APT (Advanced Persistent Threat)

- Scenario: A prolonged and targeted cyberattack on the organization.

- Response Actions:

1. SOC Analyst detects unusual prolonged activity.

2. Conduct a deep investigation to identify and isolate the threat.

3. Engage a specialized cybersecurity team if necessary.

4. Strengthen long-term security measures.

5. Document the incident.

- Time Frame for Action: Initial response within 1 hour.

- Owner: ISO

- Risk Reports to: CTO

15. Unpatched Vulnerability

- Scenario: An attacker exploits an unpatched software vulnerability.

- Response Actions:

1. SOC Analyst identifies the exploitation attempt.

2. Apply the necessary patches immediately.

3. Conduct a vulnerability assessment.

4. Ensure regular patch management protocols.

5. Document the incident.

- Time Frame for Action: Patching within 24 hours.

- Owner: ISO

- Risk Reports to: CTO

16. Third-Party Vendor Breach

- Scenario: A data breach occurs at a third-party vendor.

- Response Actions:

1. ISO communicates with the vendor to understand the breach.

2. Assess the impact on the company’s data.

3. Notify affected parties if necessary.

4. Review and possibly terminate the vendor contract.

5. Document the incident.

- Time Frame for Action: Assessment within 48 hours.

-

Owner: ISO

- Risk Reports to: CTO

17. Wireless Network Compromise

- Scenario: Unauthorized access to the company's wireless network.

- Response Actions:

1. SOC Analyst detects the unauthorized access.

2. Block the intruding device.

3. Change wireless network passwords and enhance security.

4. Perform a network security assessment.

5. Document the incident.

- Time Frame for Action: Blocking within 30 minutes.

- Owner: SOC Analyst

- Risk Reports to: CTO

18. Physical Security Breach

- Scenario: Unauthorized person gains physical access to a secure area.

- Response Actions:

1. ISO coordinates with physical security to remove the intruder.

2. Assess any potential damage or theft.

3. Review and enhance physical security measures.

4. Document the incident.

- Time Frame for Action: Intruder removal within 15 minutes.

- Owner: ISO

- Risk Reports to: CTO

19. Compromised Email Account

- Scenario: An employee's email account is hacked.

- Response Actions:

1. SOC Analyst identifies the compromise.

2. Immediately reset the email account password.

3. Review email logs for suspicious activity.

4. Conduct a security awareness refresher for the employee.

5. Document the incident.

- Time Frame for Action: Password reset within 10 minutes.

- Owner: SOC Analyst

- Risk Reports to: CTO

20. Cloud Service Breach

- Scenario: An attacker gains access to the company's cloud services.

- Response Actions:

1. SOC Analyst detects and revokes unauthorized access.

2. Conduct a full audit of the cloud services.

3. Strengthen cloud security configurations.

4. Notify affected parties if necessary.

5. Document the incident.

- Time Frame for Action: Revocation within 30 minutes.

- Owner: SOC Analyst

- Risk Reports to: CTO

These scenarios, along with their corresponding response actions, time frames, and ownership, form a comprehensive Incident Response Playbook. This ensures a rapid, efficient, and structured response to various cyber threats, maintaining the integrity and security of our information assets.

**7. Incident Classification**  
Incident Classification is critical for effective risk management. This section will be enhanced with a detailed classification matrix that considers the potential impact on confidentiality, integrity, and availability (CIA) of information assets. We will discuss how incidents are categorized based on their risk profile and the compliance implications of each category.

Governance principles will guide the classification process, ensuring that it aligns with the organization’s risk appetite and incident response strategy. This will aid in prioritizing incidents and allocating resources efficiently.

**8. Incident Reporting**  
Incident Reporting is a cornerstone of both governance and compliance. This section will be expanded to include protocols for internal and external reporting, detailing the channels for communication and the thresholds for reporting incidents to authorities in line with regulatory requirements.

We will emphasize the importance of timely and accurate reporting for risk management, ensuring that the organization can respond effectively to mitigate the impact of incidents.

**9. Incident Assessment**  
Incident Assessment is where risk management comes to the forefront. This section will be elaborated to describe the methodologies for assessing the risk associated with an incident, including the tools and techniques used to evaluate the potential business impact.

Compliance considerations will also be addressed, outlining how the assessment process helps to ensure that the organization’s response is in line with legal and contractual obligations.

**10. Incident Containment**  
Incident Containment strategies are essential for managing the risks associated with security incidents. This section will be expanded to discuss containment measures in detail, considering the governance structures that support decision-making during an incident.

We will also cover the compliance aspects of containment, such as the legal implications of isolating systems and the importance of adhering to privacy regulations while handling personal data during an incident.

**11. Incident Eradication**  
Incident Eradication focuses on eliminating the threat and reducing the risk to the organization. This section will be enhanced with procedures that align with the organization’s risk management policies, discussing the techniques for thoroughly removing threats from the environment.

Governance and compliance will be considered in the context of eradication efforts, ensuring that actions taken are authorized, documented, and in accordance with all relevant regulations.

**12. Incident Recovery**  
Incident Recovery is a critical phase where risk management strategies are implemented to restore normal operations. This section will be expanded to include recovery plans that consider the organization’s risk tolerance and the need to maintain compliance during the recovery process.

We will discuss the governance aspects of recovery, such as the roles and responsibilities of management and the IRT in overseeing the recovery efforts and ensuring that business objectives are met.

**13. Post-Incident Analysis**  
Post-Incident Analysis is an opportunity for governance and risk management to drive continuous improvement. This section will be elaborated to include a comprehensive review process that evaluates the organization’s response to an incident and identifies opportunities to enhance risk management practices.

Compliance lessons will also be a focus, with discussions on how the analysis can inform updates to policies and procedures to better meet regulatory requirements.

**14. Training and Awareness**  
Training and Awareness programs are key to managing the human element of risk. This section will be expanded to include a detailed training curriculum that covers governance, risk management, and compliance topics, ensuring that all employees are equipped to handle incidents in line with the organization’s policies.

We will discuss how ongoing awareness initiatives contribute to a culture of compliance and risk-awareness, reducing the likelihood of incidents and improving the overall security posture.

**15. Review and Maintenance**  
Review and Maintenance ensure that the playbook remains a relevant and effective tool for governance, risk management, and compliance. This section will be expanded to outline the processes for regularly reviewing and updating the playbook, incorporating feedback from incidents, changes in the threat landscape, and evolving regulatory requirements.

We will discuss the governance structures that oversee the review process, ensuring that the playbook continues to support the organization’s strategic objectives and risk management framework.

**7. Incident Classification**  
Incident Classification is critical for effective risk management. This section will be enhanced with a detailed classification matrix that considers the potential impact on confidentiality, integrity, and availability (CIA) of information assets. We will discuss how incidents are categorized based on their risk profile and the compliance implications of each category.

Governance principles will guide the classification process, ensuring that it aligns with the organization’s risk appetite and incident response strategy. This will aid in prioritizing incidents and allocating resources efficiently.

**8. Incident Reporting**  
Incident Reporting is a cornerstone of both governance and compliance. This section will be expanded to include protocols for internal and external reporting, detailing the channels for communication and the thresholds for reporting incidents to authorities in line with regulatory requirements.

We will emphasize the importance of timely and accurate reporting for risk management, ensuring that the organization can respond effectively to mitigate the impact of incidents.

**9. Incident Assessment**  
Incident Assessment is where risk management comes to the forefront. This section will be elaborated to describe the methodologies for assessing the risk associated with an incident, including the tools and techniques used to evaluate the potential business impact.

Compliance considerations will also be addressed, outlining how the assessment process helps to ensure that the organization’s response is in line with legal and contractual obligations.

**10. Incident Containment**  
Incident Containment strategies are essential for managing the risks associated with security incidents. This section will be expanded to discuss containment measures in detail, considering the governance structures that support decision-making during an incident.

We will also cover the compliance aspects of containment, such as the legal implications of isolating systems and the importance of adhering to privacy regulations while handling personal data during an incident.

**11. Incident Eradication**  
Incident Eradication focuses on eliminating the threat and reducing the risk to the organization. This section will be enhanced with procedures that align with the organization’s risk management policies, discussing the techniques for thoroughly removing threats from the environment.

Governance and compliance will be considered in the context of eradication efforts, ensuring that actions taken are authorized, documented, and in accordance with all relevant regulations.

**12. Incident Recovery**  
Incident Recovery is a critical phase where risk management strategies are implemented to restore normal operations. This section will be expanded to include recovery plans that consider the organization’s risk tolerance and the need to maintain compliance during the recovery process.

We will discuss the governance aspects of recovery, such as the roles and responsibilities of management and the IRT in overseeing the recovery efforts and ensuring that business objectives are met.

**13. Post-Incident Analysis**  
Post-Incident Analysis is an opportunity for governance and risk management to drive continuous improvement. This section will be elaborated to include a comprehensive review process that evaluates the organization’s response to an incident and identifies opportunities to enhance risk management practices.

Compliance lessons will also be a focus, with discussions on how the analysis can inform updates to policies and procedures to better meet regulatory requirements.

**14. Training and Awareness**  
Training and Awareness programs are key to managing the human element of risk. This section will be expanded to include a detailed training curriculum that covers governance, risk management, and compliance topics, ensuring that all employees are equipped to handle incidents in line with the organization’s policies.

We will discuss how ongoing awareness initiatives contribute to a culture of compliance and risk-awareness, reducing the likelihood of incidents and improving the overall security posture.

**15. Review and Maintenance**  
Review and Maintenance ensure that the playbook remains a relevant and effective tool for governance, risk management, and compliance. This section will be expanded to outline the processes for regularly reviewing and updating the playbook, incorporating feedback from incidents, changes in the threat landscape, and evolving regulatory requirements.

We will discuss the governance structures that oversee the review process, ensuring that the playbook continues to support the organization’s strategic objectives and risk management framework.