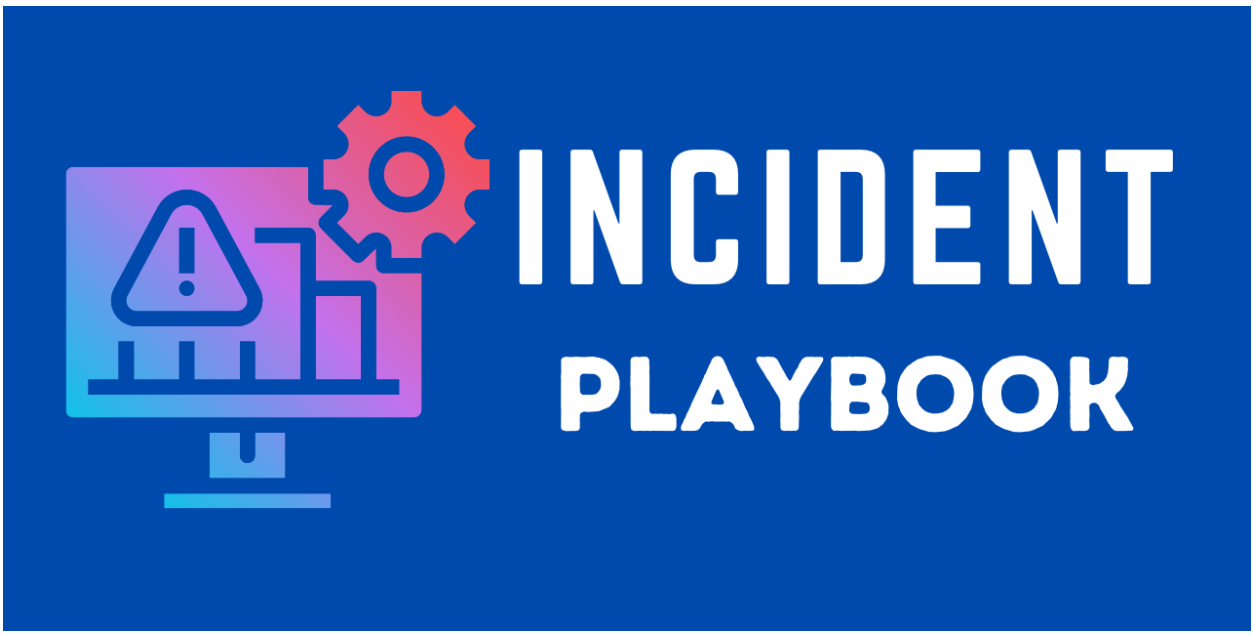
Disaster Recovery Playbook for Rove Hotels



Assignment 4

Scenario: Web defacement on Rove Hotel Website

Gregory Stephens

Executive Summary

This playbook provides a structured response and recovery guide for incidents involving web defacement. It outlines roles, responsibilities, and detailed procedures across each phase of the incident lifecycle, from detection to post-incident review.

Ownership and Approval

CSIRP Owner and Title	Phone	Email	Date	Signature
Henry Pog *CISO*	202-673-9319	henrypog@rovehotels.com	2025-04-18	
Approved By	**Phone**	**Email**	**Date**	**Signature**
Doug Fir	202-298-5700	Dougfir@rovehotels.com	2025-04-18	

Revision History

Showing current and the three previous major revisions of this document.

Version	Description	Revision Date	Review Date	Reviewer Name
1.0	Creation of document	2022-04-29	2022-04-29	Henry Pog
1.1	Adding of CISO title to owner	2022-04-30	2022-04-30	Henry Pog
1.2	Adding Lost or Stolen Equipment	2022-04-31	2022-04-31	Henry Pog
1.3	Added referral to the Login Credentials Compromised	2022-05-05	2022-05-05	Henry Pog

1. Incident Identification and Reporting

This section focuses on detecting and confirming the web defacement incident.

Questions:

- How was the web defacement detected? (e.g., customer complaint, internal monitoring, external notification)
- What is the timestamp of the incident?
- Who reported the incident? (internal team, customer, third-party vendor, etc.)
- What evidence supports the identification of the web defacement? (screenshots, logs, etc.)

- Is there an initial assessment of the scope and impact of the defacement?
- Was the incident reported to the appropriate internal teams (e.g., IT, security, legal)?

Name	Email or Phone Number
Network Operations	netops@rovehotels.com
Help Desk	helpdesk@rovehotels.com
Email Support	emailsup@rovehotels.com
Security Operations	secops@rovehotels.com, 202-885-5600
Human Resources	hr@rovehotels.com
Legal Services	legal@rovehotels.com

2. Initial Response and Containment

This section outlines the immediate actions to prevent further damage.

Questions:

- Has the affected website been taken offline or isolated to prevent further exposure?
- Are backups of the website available and intact?
- Have logs been preserved for forensic analysis?
- What measures are being taken to prevent unauthorized access to other systems?
- Who is responsible for coordinating the initial response?
- Are there any known indicators of compromise (IOCs) associated with the defacement?

3. Assessment and Analysis

This section involves understanding the root cause and extent of the incident.

Questions:

- What was the method used to deface the website? (e.g., SQL injection, XSS, unauthorized admin access)
- Were any vulnerabilities exploited to gain access? If so, which ones?
- What content was altered or replaced on the website?
- Was sensitive data (e.g., customer information, payment details) exposed or stolen?
- Are there any signs of lateral movement or additional compromised systems?
- What tools or techniques were used by the attacker?

4. Communication Plan

This section ensures proper communication with stakeholders during the incident.

Questions:

- Who are the key stakeholders that need to be informed? (e.g., senior management, PR team, customers)
- What is the timeline for notifying affected parties?
- What is the messaging strategy for public communication? (e.g., press release, social media updates)
- Are there legal or regulatory obligations to report the incident? (e.g., GDPR, PCI DSS)
- How will internal teams be kept informed throughout the recovery process?
- What is the plan to address potential reputational damage?

5. Eradication and Recovery

This section focuses on removing the threat and restoring normal operations.

Questions:

- What steps are being taken to remove malicious code or unauthorized changes from the website?
- Are patches or updates being applied to address the vulnerabilities exploited?
- How will the website be restored? (e.g., from backups, manual reconfiguration)
- What testing will be performed to ensure the website is secure before going live again?
- Are there any residual risks after recovery? If so, how will they be mitigated?
- Who is responsible for signing off on the recovery process?

6. Post-Incident Review and Lessons Learned

This section evaluates the response to improve future incident handling.

Questions:

- What were the strengths and weaknesses of the response effort?
- Were all steps in the DR Playbook followed effectively?
- What could have been done differently to minimize the impact of the incident?
- Are there any gaps in the current security posture that need to be addressed?
- What training or resources are needed to better prepare for similar incidents in the future?
- Should the DR Playbook be updated based on lessons learned?

7. Documentation and Reporting

This section ensures that all aspects of the incident are documented for accountability and compliance.

Questions:

- Has a detailed incident report been created, including timelines, actions taken, and outcomes?

- Are all communications related to the incident documented?
- Have logs, screenshots, and other evidence been securely stored for future reference?
- Is there a record of all personnel involved in the response effort?
- Will the incident be reported to relevant authorities or regulatory bodies?
- What metrics will be used to measure the effectiveness of the response?

8. Preventive Measures and Continuous Improvement

This section focuses on preventing recurrence and enhancing security.

Questions:

- What additional security controls will be implemented to prevent web defacement? (e.g., WAF, file integrity monitoring)
- Are regular vulnerability assessments and penetration tests scheduled for the website?
- Will employee training on cybersecurity best practices be updated or expanded?
- Are there plans to implement multi-factor authentication (MFA) for administrative access?
- How will the organization monitor for signs of future attacks?
- What is the long-term strategy for maintaining website security?

References

- https://cloudian.com/guides/disaster-recovery/4-disaster-recovery-plan-examples-and-10-essential-plan-items/
- https://www.atlassian.com/incident-management/itsm/disaster-recovery-plan-examples