Playbook for Cat & Box Scenario

Prepared by: Mahad Mohamood

Date: July 31, 2024

Table of Contents

Executive Summary

This report presents a comprehensive playbook for Box Manufacturing to effectively manage data breaches.

According to IBM, "a data breach is any security incident in which unauthorized parties access sensitive or confidential information, including personal data (Social Security numbers, bank account numbers, healthcare data) and corporate data (customer records, intellectual property, financial information). "

The playbook defines procedures and guidelines for detecting, preventing, and responding to data breaches, ensuring a well-coordinated response.

It includes the roles and responsibilities of the incident response team, a detailed workflow for managing breaches, communication strategies, and steps for containment, eradication, and post-incident review.

Key players and their roles

In this organization, we have a non-technical management response team and an Incident Response Team (IRT) that handles the technical aspects of data breaches.

The Incident Response Team (IRT) updates management on incidents, actions taken, and next steps, keeping them informed and answering to them.

According to NIST, an incident response team is "group of individuals usually consisting of Security Analysts organized to develop, recommend, and coordinate immediate mitigation actions for containment, eradication, and recovery resulting from computer security incidents."

The non-technical management response team

1. Mr. Percy F: CEO of Box

Role: Oversees the organization and is informed of major highlights and impacts from data breaches.

Expectation: Requires regular updates on the status and impact of the incident, relying on detailed information from the response team.

2. Miss Misha F: Shift and Production Manager

Role: Acts as the point of contact for Mr. Percy F., providing him with executive summaries and actionable items.

Expectation: Responsible for communicating critical information and updates about the breach to Mr. Percy F.

The incident response team

1. SOC (Security Operations Center)

Role: Monitors Box's network, systems, and data for security incidents.

Expectation: Identifies and reports breaches to Cat, providing detailed technical information necessary for addressing the breach.

2. Cat (Consultant at MSSP)

Role: Manages overall security for Box, oversees incident response and approves all related playbooks and workflows.

Expectation: Receives detailed breach information from SOC, manages the response process, and coordinates with third parties.

3. Me (Specialist)

Role: Develop and document playbooks and workflows for data breach incidents.

Expectation: Creates comprehensive and effective documents to be reviewed and approved by Cat, ensuring all aspects of the breach response are covered.

Triggers

Some events may serve as catalysts for initiating an investigation into a potential data breach.

When analyzing a particular trigger event / catalyst the following questions should always be asked :

- What systems or data have been affected?
- What is the scope of the breach ?
- How can we prioritize response efforts based on affected assets ?

Now lets take the following triggers into consideration.

1. Alerts from Security Tools

Automated alerts from :

- intrusion detection systems (IDS)
- intrusion prevention systems (IPS)
- antivirus software

Questions:

- What type of alert was generated (e.g., virus detection, intrusion attempt)?
- What was the severity level of the alert?

2. User Reports

Reports from employees or users about unusual system behavior.

Questions:

- What specific issues or anomalies did the user report?
- When did the user first notice the problem ?
- How frequently is it occurring?

3. Anomalous System Behavior

Irregularities such as system crashes, slow performance, or unexplained errors.

Questions:

- What types of anomalies are being observed (e.g., crashes, slowdowns)?
- Have there been recent changes or updates to the system that might explain the behavior?

4. Unauthorized Access Attempts

Multiple failed login attempts or unauthorized access by users.

Questions:

- What are the specifics of the unauthorized access attempts (e.g., IP addresses, times)?
- Have any successful unauthorized accesses been detected, and if so, which systems or data were accessed?

5. Data Exfiltration Signs

Unusual data transfers or outbound connections.

Questions:

- What data was being transferred, and where was it being sent?
- Was the data transfer authorized, or does it appear to be part of an unauthorized activity?

6. System and Application Logs

Anomalies or irregularities in logs.

Questions:

- What anomalies or irregularities are present in the logs?

- Have there been any recent logins or access attempts that are unusual or unauthorized?

7. Third-Party Security Incidents

Notifications from third-party vendors about security incidents.

Questions:

- What details are available about the third-party incident, and how does it relate to our systems?
- Are there any recommended actions or precautions provided by the third-party vendor?

Workflow

The following steps delineate the thorough and detailed actions that should be undertaken to effectively manage and address a potential data breach.

1. Detection

SOC identifies unusual activity or confirms a data breach.

Questions :

- What is the nature of the suspicious activity?
- How was the breach detected?

2. Notification

Immediate alert to Cat and relevant internal personnel to initiate response procedures.

3. Assessment

Evaluate the scope and impact of the breach.

Questions :

- What is the extent of data compromise?
- Which systems are affected?
- What vulnerabilities were exploited?

4. Containment

Implement measures to prevent further data loss.

Questions :

- Have malicious activities been blocked ?
- Have affected systems been isolated to prevent further data compromise ?

5. Eradication

Remove the threat from the environment.

Questions :

- What steps are needed to remove malicious elements?

- Have all vulnerabilities been addressed?

6. Recovery

Restore systems and data to normal operations.

Questions :

- Which systems need to be rebuilt, and what specific steps are required for each system?
- How will we verify the integrity of the restored data to ensure it has not been tampered with or corrupted?

7. Post-Incident Review

Analyze the breach to understand its causes and the effectiveness of the response.

Questions :

- How did the breach occur?
- What was the effectiveness of the response?
- What strategies can we implement to prevent future breaches and improve our response protocols?
- How can we verify that the network and systems are secure and have not been compromised?
- What comprehensive scans are necessary to detect any remnants of the breach, and how will they be performed?

Communication

This section contains sample letters: a non-technical letter addressed to the management team and a technical letter addressed to the Incident Response Team (IRT).

Technical Letter to 3rd Party Provider

Subject: Urgent: Data Breach Notification and Request for Assistance

Dear Cat and IT team at Box,

I am writing to inform you of a data breach that has recently occurred within our network. The incident has been detected and we are actively working to contain and remediate the situation. Given your role in managing our security needs, we need your immediate assistance and expertise to address the following:

Details of the Breach:

- Nature of the Incident: Unauthorized access to sensitive data.
- Affected Systems: [Specify affected systems]
- Detection Method: [Describe how the breach was detected]

Immediate Actions Required:

- Analysis: We require a thorough analysis to understand the scope of the breach and identify any compromised data.
- Remediation: Assistance with remediation steps to secure our systems and prevent further unauthorized access.

- Enhanced Monitoring: Implement enhanced monitoring to detect any residual threats or abnormal activities.

Thank you for your immediate attention to this matter.

Best regards,

Mahad Mohamood

Non-Technical Letter to Client

Subject: Important Update: Data Breach Incident

Dear Misha,

I hope this message finds you well. We are reaching out to inform you about a recent incident that has impacted our network security. Our systems have experienced a data breach, and we are taking comprehensive steps to address the situation.

Here are the key details and actions we are taking:

Incident Overview:

- What Happened: We detected unauthorized access to some of our systems, which may have affected certain data.
- Current Status: We are actively working with our security partners to investigate the breach and secure our systems.

Immediate Actions:

- Containment: We have contained the breach and are working to ensure no further unauthorized access occurs.
- Remediation: We are restoring affected systems and verifying the integrity of our data.
- Monitoring: Enhanced monitoring is being implemented to detect any residual issues.

Next Steps:

- Updates: We will keep you informed about the progress of our investigation and any potential impacts.
- Actions for You: At this time, there are no specific actions required from you, but we will provide guidance if needed.

We understand the importance of this matter and are committed to resolving it as swiftly as possible. If you have any questions or require further information, please do not hesitate to reach out.

Thank you for your understanding and support.

Best regards,

Mahad Mohamood

Conclusion

The playbook provides a structured approach for managing data breaches at Box Manufacturing.

By adhering to these procedures, the organization can effectively handle data breaches, mitigate their impact, and strengthen its overall security posture.

References

1. What is a data breach?. IBM. (2024, May 24). https://www.ibm.com/topics/data-breach

2. Editor, C. C. (n.d.). Computer Incident Response Team (CIRT) - glossary: CSRC. CSRC Content Editor. https://csrc.nist.gov/glossary/term/computer_incident_response_team