Data Breach Playbook for the Company (Box)

Daniel Deng

This is a fictional scenario, and all characters in it are created solely for demonstration purposes.

Table of Contents

Executive Summary:

Box, a small manufacturing company specializing in cardboard boxes for cats, has contracted Cat, a consultant from a Managed Security Service Provider (MSSP), to oversee their security needs. Box's CEO, Percy F., has employed a Security Operations Center (SOC) to monitor their network, systems, and data. Miss Misha F., the shift and production manager, is to be informed of any major incidents that may impact the business.

In the event of a potential data breach, the SOC follows a structured workflow to ensure a thorough response. The process includes detection, initial assessment, containment, notification of key personnel, investigation by designated experts, analysis and reporting, communication with stakeholders, remediation, documentation, review, and follow-up. This workflow ensures that all relevant parties are informed, and necessary actions are taken to mitigate the breach and prevent future occurrences.

To prepare for future data breach threats, we have developed a playbook for BOX that incorporates a comprehensive workflow detailing the actions required for response. Regular updates to the playbook, along with training for all involved personnel, will ensure the company remains vigilant and capable of effectively responding to any security incidents.

Potential Data Breach response Workflow

Sensitive data is a valuable asset for Box company, including their customers' payment card information (PCI) and the private data of Box's employees (PII) (PCI, n.d.). A breach of this data would significantly impact the confidentiality and integrity pillars of the CIA triad. SOCs as contractors have a structured set of processes that are carried out to ensure that security is maintained (Cherian, 2023).

- **Detection:** SOC Analyst identifies a potential data breach through Splunk alerts.
- **Initial Assessment:** SOC Analyst performs an initial assessment to confirm the legitimacy of the breach.
    - Verify the source of the breach.
    - Identify affected systems and data.
- **Containment:** SOC Analyst contains the breach to prevent further data loss.
    - Isolate affected systems.
    - Block malicious IP addresses in the firewall policy.
    - Change passwords and update access controls.

- **Notification:** SOC Analyst notifies Cat and other key personnel:
  - **Cat** (MSSP Consultant):
    - Email: cat@soc.cat
    - Phone 905-4616 or cell 902-4321
  - **Miss Misha F.** (Shift and Production Manager):
    - Email: mesha@box.cat
    - Phone 902-9836
  - **Minka F.** (Alternate):
    - Email: minka@box.cat
    - Phone 562-7658

- **Investigation:** Cat assigns specific tasks to team members based on expertise:
  - **Dusty** (Database Specialist):
    - Conduct a forensic analysis of the database to determine the extent of the breach.
    - Identify compromised data and potential vulnerabilities.
  - **Lucky** (IT Support Specialist):
    - Provide technical support and assist in system recovery.
  - **Ned** (Network Administrator):
    - Analyze network traffic and logs for evidence of breach origin.
    - Ensure network security measures are in place.

- **Analysis and Reporting:** SOC Team and Cat compile a detailed incident report:
  - Summary of the breach.
  - Systems and data affected.
  - Actions taken to contain the breach.
  - Preliminary findings from forensic analysis.

- **Communication:** SOC Team communicates with stakeholders:
  - **Miss Misha F.** (During office hours):
    - Provide a summary of the incident and potential impacts on production.
  - **Minka F.** (After office hours/weekends):
    - Provide necessary updates and coordination.
  - **Mr. Percy F.** (CEO):
    - Inform personally if the incident is escalated, urgent, or unresolved after 48 hours.

- **Remediation:** SOC Team**,** Cat and relative personnel implement remediation measures:
  - Patch vulnerabilities.
  - Restore affected systems.
  - Verify the integrity of recovered data.

- **Documentation and Review:**

  - **SOC Team** documents all actions taken and findings.
  - **Cat** reviews the incident response and provides feedback.

- **SOC Team** updates playbooks and workflows based on the incident.

- **Follow-up and continuous monitoring:**
  - SOC Team conducts a follow-up analysis to ensure no further threats.
  - Cat ensures all parties are informed of the incident resolution

Trigger Items Affecting Incident Response Workflow

- **Data breach that involved 3rd party vendor:**
  - 3rd Party database provider (AWS, Azure, etc.) will be involved to aid the investigation and data restoration.
- **Are the breached data very sensitive or critical:**
  - If so, Percy as the CEO should be involved. Helping makes decisions on the remediation process.
- **The incident has not been solved for 48 hours:**
  - Cat should work with SOC and other incident response team members to properly respond to the incident within 48 hours, if not. Percy should be informed and involved.
- **A persistent attack:**
  - If the attack is persistent, During the Containment phase in the workflow: the SOC Analyst should also invite other key personnel (Cat, Dusty, Lucky, Ned) to work together and contain the breach to prevent further data loss.
  - Also combine the Notification phase of the workflow if the attack is persistent. Making sure everyone involved is on the same page and preventing further attacks.

Client PlayBook for potential future Data Breach

A data breach is a security violation, in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen, altered, or used by an individual unauthorized to do so. A Data Breach Playbook serves as a comprehensive guide to effectively respond to potential data

loss incidents within our organization. This playbook can be used as a template that outlines the steps and procedures that Box company must follow to detect, assess, contain, and mitigate data loss events promptly and minimize their impact on sensitive information (CyberAlberta, 2024).

Security team in place: Dusty, Ned, and Lucky as the security team of the Box company, should always be in place when an incident is detected.

Isolation and policy update: Isolate all affected systems or accounts from the infrastructure (internal network and external 3rd party cloud like AWS S3) to prevent further data exfiltration. Block the associated attack IP in our firewall policy.

Impact identification: Review the impact of the data breach based on the CIA triad. Identify the most valuable data.

Incident report: Provide an interim incident report to the affected system(s) service owners or key personnel, in our case: Cat and Percy.

Preserve evidence: Preserve any compromised assets or copies, if possible, for future analysis including forensic investigation, SOC and Dusty should be in charge.

Remediation plan: Incorporate technical and business analysis in developing a prioritized remediation plan which includes a communication strategy.

Restoration: Conduct a restoration of any compromised systems from a trusted and tested backup. The priority of recovery of these systems will be based on business impact analysis and business criticality

System re-imaged and continuous monitoring: Complete malware scanning of environment systems, Continue to monitor for signatures and other indicators of compromise to prevent the malware attack from re-emerging.

Secure data both in transit and at rest: Upgrade company security policy and consider using encryption to protect valuable and sensitive data. Use Cloud providers such as AWS, or Azure to leverage their default data encryption to protect data in transit and at rest (AWS, n.d.).

Technical letter to 3rd party provider

To: Cat (MSSP & 3rd Party provider involved (AWS, Azure, etc.))
From: Daniel Deng (SOC Specialist)
Date:

Critical Data Breach Detected

Hello Cat,

I hope you are well. I am reaching out to notify you of a critical data breach incident discovered within Box Manufacturing's database. Below is a quick report about the detailed findings and the urgent actions needed.

Incident:

Detection Time:
Affected data: (List the breached data and sensitive information here)
Impact: (Impact on Confidentiality and Integrity of CIA triad)

Our Action Taken:

The SOC team and Ned, our Network Administrator, have isolated the affected systems to prevent further spread.

Dusty, the database specialist, is conducting a forensic analysis of the database to determine the extent of the breach, in addition, he is working with 3rd party database provider to restore the data.

Misha, the shift and production manager, has been notified to manage any production impacts. Minka, her alternate, has also been informed in case of after-hours/weekend coordination.

MSSP coordination:

We need to further investigate this incident regarding the source and impact, we may need your coordination and communication between different key personnel. In addition, we need to draft a comprehensive incident report in case we need to notify Percy. Furthermore, a detailed remediation and recovery plan needs to be drafted to promote the data restore process.

Best regards,

Daniel Deng

SOC Specialist for Box Manufacturing

Non-technical letter to the client

To: Affect client name
From: Box Company
Date:

Notification of privacy incident

Dear [affected client's name],

We are writing to let you know about a potential recent privacy breach that involved some of your information. This letter will explain what happened, how we have responded, and what it means for you.

What happened?

[On/between] [date/time period], we detected a potential attack against our database, and we believe some privacy information has been breached during this incident. We have shut down and isolated the database network immediately and no further data breach has been found.

What information was affected?

Based on our investigation, we understand that your personal information that has been affected by this incident includes:

[List the personal information affected].

What have we done in response to the breach and what does this mean to you?

Our team has successfully contained the affected network, and no further data breach has been found. All data lost has been successfully restored and privacy data leaked in transit has been encrypted with Microsoft Azure standard SHA-256 encryption. A detailed incident report can be found in this link: [incident report for client URL]

The data has been encrypted during the transit; therefore, we do not foresee any further harm to you. However, please carefully review the information that was affected by this incident and think about whether this could result in you experiencing any harm. Here are some tips:

- Be aware of emails and telephone calls from people requesting your personal details, (especially things like your date of birth, residential address, email address, username, or passwords which are often used to verify your identity).

- Change your password on your banking account.

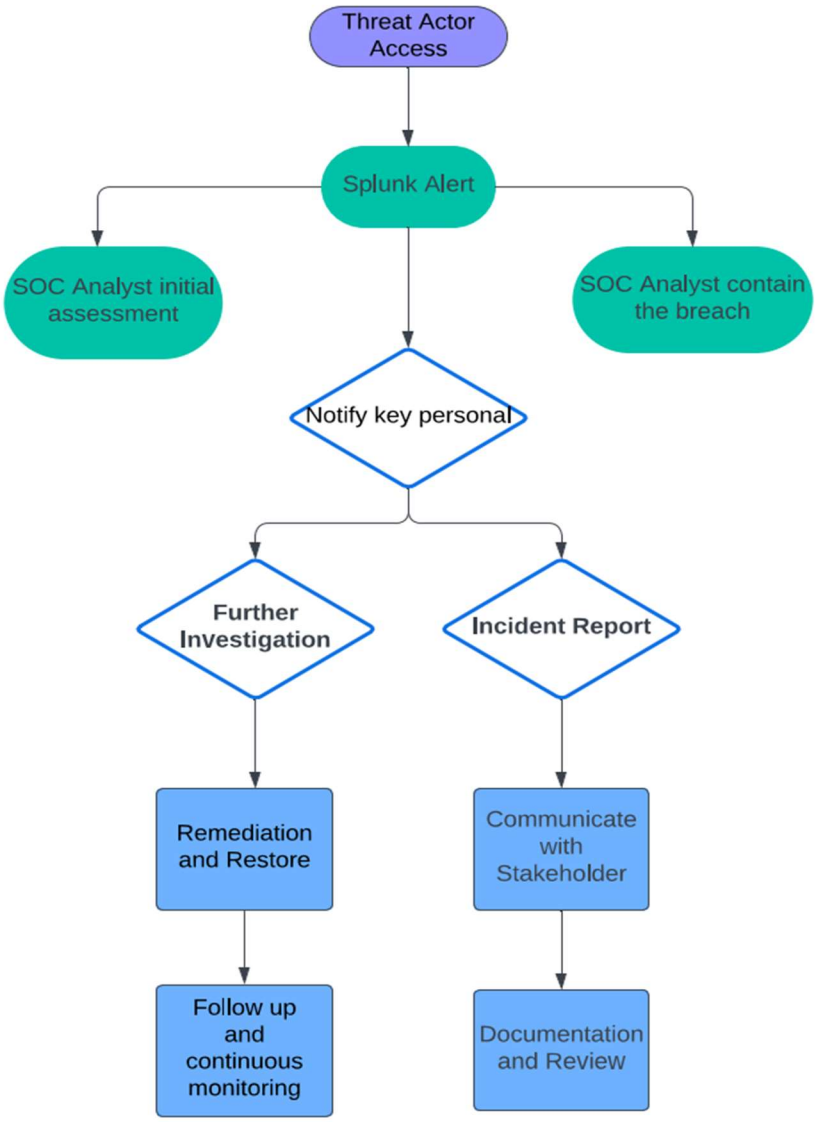
More information and making a complaint

If you have any concerns about what has happened or would like further information, you can contact: [Box company number]

Yours sincerely,

Box Company

Flow chart



References:

AWS. (n.d.). Retrieved from Encrypting Data-at-Rest and Data-in-Transit: https://docs.aws.amazon.com/whitepapers/latest/logical-separation/encrypting-data-at-rest-and--in-transit.html

Cherian, S. (2023, Oct). Retrieved from Understanding SOC Operations and Processes: https://www.micromindercs.com/blog/soc-operations-and-processes#:~:text=The%20SOC%20process%20in%20cybersecurity%20involves%20continuously%20monitoring%20network%20activities,threats%20and%20maintain%20network%20integrity.

Commissioner, O. o. (n.d.). Retrieved from Template for notifying individuals of a breach: https://ovic.vic.gov.au/wp-content/uploads/2021/06/Template-for-notifying-affected-individuals-about-a-data-breach.docx

CyberAlberta. (2024, March 13). Retrieved from Data Breach: https://cyberalberta.ca/system/files/data-breach-playbook.pdf

PCI. (n.d.). Retrieved from PCI Security Standards Overview: https://www.pcisecuritystandards.org/standards/