Data Breach Incident Playbook

For Box Manufacturing

Table of Contents

1. Revision History

This Incident Response Plan has been updated as follows:

Date	Version	Modification	Modifier
2024-10-13	1.0	Initial version established	Sumit

2. Testing & Review Cycle

To ensure the Cyber Security Incident Response Team (CSIRT) is well-informed of its responsibilities, annual testing of the Incident Response Plan is essential. In the absence of real incidents that fully engage the process, testing can be conducted through walkthroughs and practical simulations of possible incident scenarios.

1. **Annual Testing**: The Incident Response Plan will undergo testing at least once a year.
2. **Evaluation of Response**: The testing will evaluate the organization's response to potential incident scenarios, identifying any gaps in processes and areas that require enhancement.
3. **Record of Insights**: The CSIRT will record insights gained during testing, noting any steps that were executed poorly or misunderstood by participants, as well as aspects that require improvement.
4. **Plan Updates**: The Incident Handler will be responsible for updating the Incident Response Plan and distributing it to CSIRT members as needed.

3. Purpose & Scope

3.1 Purpose

This Incident Response Plan ensures Box is prepared to effectively manage data breach incidents. With cyber threats becoming more frequent and sophisticated, it's vital for Box to have a structured approach to respond swiftly to any breaches, as well as to prevent and detect them. By implementing this plan and conducting regular training, Box aims to minimize the impact of incidents, quickly contain damage, and mitigate risks.

This document outlines how Box will respond to data breaches, detailing team structures, roles, responsibilities, and processes for preparation, identification, containment, eradication, recovery, and post-incident analysis.

3.2 Scope

This plan applies to all of Box's networks, systems, data, and stakeholders, including employees, contractors, and third-party vendors. Members of the Cyber Security Incident Response Team (CSIRT) are expected to lead the response efforts. All team members should be familiar with this plan and ready to collaborate to minimize the impact of data breaches.

This document provides a framework for handling data breach incidents but does not list every possible action to address such incidents.

4. Authority

The responsibility for the security of Box's and its customers' data rests with **Mr**. **Percy F.**, the CEO. During significant cyber security incidents, such as data breaches, this responsibility will be delegated to **Miss Misha F.**, the Shift and Production Manager, ensures a swift and organized response to mitigate risks and protect sensitive information.

5. Definitions

The following definitions, as well as the incident response plan template, are based on the guidelines from Innovation, Science and Economic Development Canada [2].

- **Acceptable Interruption Window**: The time within which basic functionality must be restored for critical systems in Box.
- **Confidentiality**: Classification of sensitive data, including personally identifiable information relevant to Box's operations.
- **Cyber Security Event**: An observable occurrence affecting Box's systems or networks, such as user activity or service requests.
- **Cyber Security Incident**: Any event impacting the confidentiality, integrity, or availability of Box's information or systems, including unauthorized access or data breaches.
- **Denial of Service (DoS)**: An attack aimed at making Box's services unavailable by overwhelming them with requests.
- **Exploit**: Software or commands that take advantage of vulnerabilities in Box's systems.
- **Indicators of Compromise (IoCs)**: Forensic clues in Box's network or systems indicating a potential cybersecurity attack.
- **Integrity**: Assurance of data accuracy and consistency throughout its lifecycle in Box.
- **Maximum Tolerable Downtime**: The longest period Box can function without critical processes before risking survival.
- **Response Playbook**: A set of prescriptive measures and best practices for enhancing Box's cybersecurity posture.
- **Service Availability**: The measure of how often Box's systems are accessible and responsive to users.
- **Service Level Agreement (SLA)**: A guarantee of service availability, outlining financial repercussions if standards are not met.
- **Stakeholder Relationship Map**: A diagram depicting relationships among individuals in Box, used for IT risk assessments.
- **Vulnerability**: A bug or weakness in Box's systems that can be exploited for malicious purposes.
- **War Room**: A designated space for managing major incidents involving Box's cybersecurity.
- **Zero-Day**: A vulnerability known to Box's software vendor without an available fix, posing an exploit risk.

6. How to Recognize a Data Breach Incident

Identifying a data breach incident within Box is crucial for ensuring the integrity and security of sensitive information. According to NIST, the identification process involves two key components: **leads** and **indicators** [3].

1. **Leads**: These are proactive signs that suggest a potential breach may have occurred or is in progress. For Box, relevant leads may include:
    - **Web Server Logs**: Unusual patterns in web server logs that suggest attempts to exploit vulnerabilities within Box's manufacturing and distribution networks.
    - **Security Vulnerability Searches**: Any detected searches targeting Box's network, which may indicate reconnaissance by potential attackers.
    - **Attack Notifications**: Alerts from cybersecurity tools indicating that a breach attempt or malicious activity has been detected.
2. **Indicators**: These are reactive signs that suggest a breach has already occurred. Important indicators for Box to monitor include:
    - **Suspicious Emails**: Returned emails with unusual content, which may indicate phishing attempts targeting employees.
    - **Unauthorized Login Attempts**: Multiple failed login attempts from unfamiliar IP addresses or unknown networks, signaling possible unauthorized access.
    - **Cache Overflows**: Monitoring database servers for cache overflows, which can indicate malicious data retrieval attempts.

By recognizing both leads and indicators, Box can enhance its ability to detect and respond to data breaches effectively, ensuring the protection of its sensitive data and maintaining trust with customers and partners .

7. Cyber Security Incident Response Team (CSIRT) for Data Breach Incidents at Box Manufacturing

7.1 CSIRT Structure

The following roles are established within Box's CSIRT for handling data breaches:

CSIRT Role	Role Definition
Executive	**Mr. Percy F. (CEO)**: Responsible for overall cyber security, reporting to the board and overseeing critical decisions regarding data breaches.
Incident Handler	**Cat (MSSP Consultant)**: The primary contact for incident management, responsible for activating the Incident Response Plan and overseeing remediation efforts.

Communications Expert	**Miss Misha F. (Shift and Production Manager)**: Acts as the primary liaison for incident communications, ensuring relevant stakeholders are informed of incidents and their potential impact.
Note-taker	**Miss Minka F. (Alternate Manager)**: Documents all incident-related communications and meetings, maintaining records for analysis and post-mortem evaluations.
Database Specialist	**Dusty**: Provides insights into database security and integrity, assessing risks associated with potential breaches.
IT Support Specialist	**Lucky**: Offers technical support for systems impacted by data breaches, ensuring prompt recovery and security measures.
Network Administrator	**Ned**: Monitors network security and investigates any breaches affecting network infrastructure.
Legal Technician	Legal Counsel: Advises on legal implications and compliance during incidents, ensuring the organization meets regulatory requirements.

7.2 CSIRT Responsibilities

Executive Responsibilities

1. **Mr. Percy F.**:
    1. Oversees the CSIRT and is informed of escalated or unresolved incidents after 48 hours.
    2. Engages with the board of directors to discuss security needs and impact of incidents.

Incident Handler Responsibilities

1. **Cat**:
    1. Activates the Incident Response Plan upon detection of a data breach.
    2. Coordinates with the SOC to ensure immediate actions are taken to mitigate threats.
    3. Provides detailed incident reports and remediation plans to the appropriate stakeholders, including Percy and Misha.

Communications Expert Responsibilities

- **Miss Misha F.**:

    1. Ensures timely communication regarding data breaches to internal and external stakeholders.
    2. Updates Percy on significant incidents that may impact business operations.

Note-taker Responsibilities

- **Miss Minka F.**:

    1. Maintains accurate documentation of all incident-related meetings and communications.
    2. Assists in compiling post-mortem reports to identify lessons learned.

Database Specialist Responsibilities

- **Dusty**:

    1. Assesses potential impacts on database security during data breaches.
    2. Collaborates with Cat to analyze data integrity and suggest recovery procedures.

IT Support Specialist Responsibilities

- **Lucky**:

    1. Provides technical support during incidents, focusing on restoring operations.
    2. Works closely with Cat to implement security measures and prevent future breaches.

Network Administrator Responsibilities

- **Ned**:

    1. Monitors network activity for suspicious behavior that may indicate a breach.
    2. Engages in forensic analysis to determine the scope and impact of data breaches.

All Staff Responsibilities

- All employees must be familiar with the procedures for identifying and reporting data breaches.
- Staff are instructed to report any suspicious activity to the Incident Handler or a CSIRT member immediately.

8. Contact Information

8.1 CSIRT Contacts

CSIRT Role / Title	Name	Availability	Phone	Email
CEO	Mr. Percy F.	Urgent need only		percy@box.cat
Incident Handler / MSSP Consultant	Cat	Daytime, after hours and weekend	905-4616(daytime), 902-4321(after hour and weekend)	cat@soc.cat
Communications Expert / Shift and Production Manager	Miss Misha F.	9 AM to 5 PM AST weekdays	902-9836	mesha@box.cat

Note-taker / Alternate Manager	Miss Minka F.	After hours and during weekends	562-7658	minka@box.cat

8.2 External Contacts

Role	Organization	Name	Phone	Email
Database Specialist	MSSP	Dusty	462-8952	dusty@box.cat
Network Administrator	MSSP	Ned	877-4332	ned@box.cat
IT Support Specialist	MSSP	Lucky	269-5466	lucky@box.cat

9. Incident Severity Matrix

The Incident Severity Matrix for Box Manufacturing is used by the Cyber Security Incident Response Team (CSIRT) to assess the severity of a data breach or security incident. The CSIRT, along with Cat (the MSSP consultant), will use this matrix to guide the response based on the severity of the breach.

Key Considerations:

1. **Scope of the Incident**: The CSIRT will evaluate whether the incident impacts a single system or multiple systems within Box's network.
    - Example: A breach impacting the production management system versus an isolated workstation.
2. **Criticality of Affected Systems**: The impact will be assessed based on how critical the affected systems are to Box's core manufacturing and business operations.
    - Example: A critical production server breach versus a sales system breach.
3. **Number of Affected Individuals or Teams**: The CSIRT will determine if the breach impacts a single person or multiple people, teams, or departments within Box.
    - Example: A breach impacting the production team and network administration versus an isolated incident involving IT support.
4. **Business Context**: The CSIRT will also consider the relevant business operations at the time of the incident. For example, the urgency might increase if the breach occurs during high-demand production periods.

Additional Factors Considered by CSIRT:

- **Magnitude of Impact**: The team will evaluate the known and potential size of the breach, whether the incident is contained, or if there is a risk of it spreading.
- **Likelihood of Spread**: The CSIRT will assess the risk of the breach spreading across other systems or departments and the pace at which this may occur.
- **Potential Damage**: The incident's potential impact on Box's financial position, reputation, and production capabilities will be considered.

Threat Characteristics:

The breach may stem from various sources, such as:

- **Automated or manual attacks**: Automated attacks like Distributed Denial-of-Service (DDoS) or manual insider threats such as the threat of data exfiltration by USB [1].
- **Nuisance or vandalism**: Less severe incidents may involve malware or phishing scams targeting non-critical systems.

CSIRT Assessment Process:

The CSIRT will consider the following criteria when assessing the incident:

1. **Vulnerability Exploitation**: Is there evidence that a known or unknown vulnerability was exploited?
2. **Patching**: Is there a patch available to fix the vulnerability?
3. **Type of Threat**: Is this a new threat (such as a zero-day attack), or is it a known threat that can be mitigated more quickly?
4. **Effort to Contain**: What resources are required to contain and remediate the incident?

Incident Severity Categories

Category	Indicators	Scope	Action
1 – Critical	Data loss, Malware	Widespread across Box's critical systems (e.g., production servers, customer data)	Implement CSIRT, Incident Response Plan (IRP), organization-wide response, notify executive leadership (Percy)
2 – High	Exploitation of active vulnerabilities, data theft	Affects major systems (e.g., network infrastructure, financial data)	Implement CSIRT, IRP, notify all relevant stakeholders (e.g., Misha, Minka, Dusty), and organization-wide response
3 – Medium	Phishing attempts or malware with limited spread	Multiple workstations or departments (e.g., affecting production and sales)	Initiate CSIRT, IRP, notify IT support (Lucky), database specialist (Dusty), monitor incident closely
4 – Low	Malware, phishing, or suspicious activity on one host	Individual workstation or person (e.g., isolated incident with limited impact)	Notify CSIRT, monitor situation, escalate if necessary, notify Lucky and Ned for containment

This matrix helps Box assess and respond to incidents swiftly, ensuring critical systems such as production servers, databases, and customer-facing systems are prioritized. If an incident

affects a major part of Box's operations or data, it escalates to "Critical" status, triggering a comprehensive response involving the CSIRT, Cat, and Percy F.

10. Incident Handling Process

10.1 Overview

In the event of a cybersecurity incident at Box Manufacturing, a company specializing in cardboard boxes for cats, the Cyber Security Incident Response Team (CSIRT) will follow the PICERL (Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned) model. This process is tailored to protect the company's proprietary designs, manufacturing processes, and supply chain systems from cybersecurity threats [4].

10.2 Preparation

The preparation phase ensures that Box Manufacturing is ready to respond to incidents by setting up monitoring systems, defining roles, and conducting regular training.

Trigger Point:

- Monthly system checks and security updates with Cat's MSSP team.

Actions:

- Regular backups of critical data such as design files and supplier information.
- Conduct mock incident response exercises to ensure key personnel, including Misha and Ned, understand their roles during an incident.
- Ensure all security software is updated and monitoring systems are in place.

10.3 Identification

The identification phase focuses on detecting potential incidents by analyzing logs, intrusion detection systems (IDS), and network traffic.

Trigger Point:

- Alerts from IDS or firewall indicating unusual traffic or repeated failed login attempts.

Actions:

- Ned and Lucky will review system logs for anomalies, while Cat's team assists with detailed investigation of suspicious activity.
- Notify Misha immediately if any incident is detected during production hours, or escalate to Minka during off-hours.

10.4 Containment

The containment phase aims to prevent further damage by isolating affected systems or segments of the network.

Trigger Point:

- Detection of malware on a workstation used for proprietary design development.

Actions:

- Ned will isolate the affected system from the network to prevent the spread of malware.
- Immediately disable compromised accounts and lock down access to critical servers.
- Cat's MSSP team will guide the containment process, ensuring minimal disruption to production.

10.5 Eradication

The eradication phase involves removing the threat from the system and ensuring it does not reoccur.

Trigger Point:

- Confirmation of malware infection or persistent threat actor in the network.

Actions:

- Ned and Lucky will clean the affected systems, remove malware, and patch vulnerabilities.
- Conduct a thorough scan of the entire network to ensure no further threats remain.
- Verify that backups are clean and secure before restoring them.

10.6 Recovery

In the recovery phase, Box Manufacturing will restore affected systems to normal operations and ensure they are no longer compromised.

Trigger Point:

- Successful eradication of the threat and confirmation that systems are free of malware.

Actions:

- Ned and Dusty will restore systems from clean backups, ensuring all systems return to operational status.

- Monitor the network closely for 72 hours after recovery to ensure no further compromise.
- Report recovery progress to Percy if critical systems were impacted.

10.7 Lessons Learned

The lessons learned phase focuses on reviewing the incident to identify areas for improvement in the response process.

Trigger Point:

- Post-incident debrief scheduled within one week of resolving the incident.

Actions:

- Hold a review meeting with Percy, Misha, Cat, and the CSIRT to discuss what worked and what could be improved.
- Update incident response protocols based on findings.
- Use insights to improve training for Misha, Minka, and other relevant personnel, such as phishing awareness.

11. Approval

Responsible Party
The responsibility for the development, updating, and enforcement of the Incident Response Plan rests with the following individuals:

Responsible Party Name and Title	Responsible Party Signature	Version	Date
Percy F., CEO		1.0	

The Responsible Parties have reviewed the Incident Response Plan and have delegated the responsibility for mitigating harm to the organization to the Incident Handler. In the event of a high or critical data breach incident, this responsibility is entrusted to the Incident Handler or their delegate.

---

12. Incident Handler

The Incident Handler for the Box manufacturing company is Cat, the MSSP Consultant. Cat has reviewed the Security Incident Response Plan and acknowledges that, during a data breach incident, the responsibility for managing the incident is entrusted to them or their delegate.

Cat is expected to handle the incident in a manner that mitigates further exposure of the organization. This will involve following the established process, including identification, containment, eradication, recovery, and lessons learned.

Incident Handler Name and Title	Incident Handler Signature	Version	Date
Cat, MSSP Consultant		1.0	

13. References

1. MITRE ATT&CK®. https://attack.mitre.org/
2. Government of Canada, Innovation, Science and Economic Development Canada, Office of the Deputy Minister, Digital Transformation Service Sector, Digital Transformation Service Sector. Develop an Incident Response Plan: Fillable template and example. Published December 8, 2021. https://ised-isde.canada.ca/site/cybersecure-canada/en/certification-tools/develop-incident-response-plan-fillable-template-and-example
3. Fisher W. *Data Confidentiality: Detect, Respond to, and Recover From Data Breaches*.; 2024. doi:10.6028/nist.sp.1800-29
4. Cichonski P, Millar T, Grance T, Scarfone K. *Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology*.; 2012. doi:10.6028/nist.sp.800-61r2

Technical Letter to Cat (MSSP Consultant)

Dear Cat,

Subject: Data Breach Incident Response

I am writing to formally inform you of a data breach incident that has been detected within our systems. The incident was identified on [insert date of detection], and it appears to have impacted [briefly describe the affected systems or data].

Incident Details:

- **Incident Date and Time:**
- **Nature of the Incident:**
- **Affected Systems:**
- **Data Compromised:**
- **Initial Assessment:**

Immediate Actions Taken:

1. [Describe initial containment measures]
2. [Mention any steps taken to secure the environment]
3. [List any other relevant immediate actions]

Given the severity of this incident, I request your expertise to assist us in the following areas:

- Conducting a thorough investigation to determine the cause and extent of the breach.
- Implementing additional security measures to prevent future incidents.
- Developing a communication plan for stakeholders and affected parties.

Please let us know your availability for a meeting to discuss this incident further. Your prompt response is appreciated as we work to mitigate the impact of this breach.

Thank you for your assistance.

Sincerely,
[Your Name]
[Your Title]
SOC

Non-Technical Letter to Mr. Percy F. (CEO)

Dear Mr. Percy F.,

Subject: Update on Data Breach Incident

I hope this message finds you well. I am writing to inform you of a data breach incident that has occurred within our organization. We detected the breach on [insert date of detection], and I want to assure you that we are taking this matter very seriously.

Overview of the Incident:

- **Date of Detection:**
- **Affected Data:**
- **Impact:**

Actions Taken So Far:

1. We have initiated a containment strategy to prevent further unauthorized access.
2. An investigation is currently underway to understand the cause of the breach and the extent of the damage.
3. We are collaborating with our Managed Security Service Provider to enhance our security measures moving forward.

Our priority is to protect our customers and the integrity of our operations. I will keep you updated as we learn more about the incident and the steps we are taking to address it.

Please feel free to reach out if you have any questions or require further information.

Thank you for your understanding.

Best regards,
[Your Name]
[Your Title]
SOC