Incident Response Playbook for Box Manufacturing

Table of Contents

Introduction:

This report outlines the incident response playbook developed for Box Manufacturing, a small company specializing in cardboard boxes for cats. The playbook aims to provide a structured approach for handling security incidents and communicating with relevant stakeholders, including the client (Box Manufacturing) and the third-party provider (Cat - MSSP & SOC Security Oversight).

Scope:

The scope of this playbook encompasses the procedures and protocols to be followed in the event of a suspected cybersecurity breach at Box Manufacturing. It defines the roles and responsibilities of key stakeholders, including internal teams and the MSSP consultant, Cat, in responding to and mitigating the impact of security incidents. This playbook outlines the structured approach for incident identification, notification, response, and post-incident review, ensuring clear communication, effective collaboration, and timely remediation efforts. Additionally, it addresses the need for continuous improvement through ongoing training and awareness initiatives, documentation, and collaboration with external parties.

Assuming here, a unique incident could involve a sophisticated form of social engineering attack targeting Misha, the shift and production manager at Box Manufacturing. The attack could involve a meticulously crafted email containing a malicious attachment disguised as an urgent production report or an update on a critical project.

Upon opening the attachment, malware is silently installed on Misha's computer, giving attackers unauthorized access to sensitive production data, including proprietary box designs and production schedules. The attackers could then exfiltrate this data or manipulate production schedules to disrupt operations and cause financial losses for Box Manufacturing.

This incident would require not only technical remediation to remove the malware and secure Misha's computer but also a comprehensive review of security awareness training for all employees to mitigate the risk of future social engineering attacks. Additionally, enhanced email security measures and stricter access controls may need to be implemented to prevent similar incidents from occurring in the future.

1. Analysis of the scenario:

The scenario involves Box, a small manufacturing company specializing in cardboard boxes for cats, and Cat, a consultant working for a managed security service provider (MSSP) contracted by Box for security needs. Mr. Percy F., CEO of Box, has contracted a Security Operations Center (SOC) to monitor their network, systems, and data. Percy wants to be informed of any major highlights or potential impacts caused by breaches, while Miss Misha F., the shift and production manager, should be informed of any breaches as well.

Roles and Responsibilities:

- Mr. Percy F. (CEO of Box Manufacturing)
  - Overseeing the overall operations and security posture of the company.
- Miss Misha F. (Shift and production Manager)
  - Responsible for managing shift operations and production activities.
- Cat (Consultant from MSSP)
  - Overseeing security needs and coordination with the SOC.

Third Party Provider Information:

- **Provider Name**: Cat (MSSP & SOC Security Oversight)
- **Provider Contact**: Cat@soc.cat
- **Provider Contact Information**:
  - Cat: cat@soc.cat, Phone: 902 88-1234 or Cell: 902 77-4321

Communication Channels:

- Mr. Percy F.: percy@box.cat, Phone: 902 66-9999
- Miss Misha F.: misha@box.cat, Phone: 902 69-9999 (Weekdays: 9AM to 5PM AST)
- Alternate Contact Minka F.:minka@box.cat, Phone: 902 99-9999(After-hours and weekends)

Availability:

- Miss Misha F. works weekdays from 9AM to 5PM AST.
- Minka F. covers after-hours and weekends.

Escalation Protocol:

- Mr. Percy F. wants to be personally informed if an item is escalated or urgent or remains unsolved after 48 hours.

2. Standard Operation Procedure(SOP):

- Alert the SOC immediately upon detection of a potential security Breach.
- Followed predefined escalation procedures based on severity and impact assessment.
- Initiate communication protocols to notify relevant stakeholders.

3. Communication Plan:

Notification Process:

- In case of a suspected breach, Cat will notify Miss Misha F. immediately.
- Miss Misha F. will inform Mr. Percy F. if the incident is escalated, urgent, or unresolved after 48 hours.

Incident Response Playbook overview:

The incident response playbook serves as a comprehensive guide for detecting, assessing, and responding to security incidents within Box Manufacturing's network. It encompasses key phases such as preparation, identification, containment, eradication, recovery, and lessons learned. The playbook is designed to ensure a coordinated and effective response to security incidents, minimizing disruption to business operations and mitigating the impact of security threats.

Incident Response Phases:

1.Preparation:

- Ensure all incident response team members, including Cat (consultant), Miss Misha F. (Shift and Production Manager), and Mr. Percy F. (CEO), are trained and aware of their roles and responsibilities.
- Validate and update contact information for key stakeholders and external resources, including the SOC and Cat's contact details.
- Review and verify the availability and functionality of incident response tools and resources, such as monitoring systems and communication channels.
- Establish communication channels and protocols for reporting and escalating security incidents, including procedures for notifying Miss Misha F. during work hours and Cat or Minka F. for after-hours response.

2. Identification:

- Monitor security alerts and logs for indicators of compromise (IoCs) or suspicious activities on Box Manufacturing's network and systems.
- Cat, overseeing security needs, receives alerts from the SOC and conducts initial triage to determine the nature and scope of the security incident.
- Gather relevant information, such as timestamps, affected systems, and potential impact, to classify the incident based on severity and criticality.

3. Containment:

- Isolate affected systems or networks to prevent further spread of the incident, following predefined escalation procedures.
- Implement access controls or temporary measures to limit the impact of the incident on Box Manufacturing's operations.
- Preserve evidence and logs for forensic analysis and investigation to identify the source of compromise.

4. Eradication:

- Investigate the root cause of the incident to identify the source of compromise, working closely with the SOC and Cat.
- Remove or neutralize malicious presence within the environment, applying remediation measures to prevent future occurrences.
- Patch vulnerabilities or apply updates as recommended by Cat to enhance security posture and resilience against similar incidents.

5. Recovery:

- Restore affected systems and services to normal operations following successful eradication, coordinating with IT teams and Cat.
- Verify data integrity and restore from backups, if necessary, to recover lost or corrupted data.
- Communicate restoration progress and expected timelines to stakeholders, including Miss Misha F. and Mr. Percy F., to ensure transparency and minimize disruption.

6. Lessons Learned:

- Conduct a comprehensive post-incident review with key stakeholders, including Cat, Miss Misha F., and Mr. Percy F., to assess the effectiveness of the response process.
- Identify strengths, weaknesses, and areas for improvement in incident response procedures, such as communication protocols and escalation pathways.
- Document lessons learned, including successful strategies and challenges encountered during the incident, and update incident response documentation, policies, and procedures accordingly.
- Share insights and recommendations with relevant stakeholders to enhance organizational resilience against future security incidents and ensure continuous improvement in security posture.

Trigger Items Affecting Incident Response Flow:

Time/Date: Incidents occurring during Misha's work hours may be handled directly by her, while those outside of her working hours may require escalation to Minka or Cat for after-hours response. Clear definition of working hours ensures timely response and escalation protocols are followed, maintaining continuity in incident management regardless of the time of occurrence.

Severity Level: The severity of the suspected breach will determine the urgency of the response, with critical incidents requiring immediate action and escalation to Percy if necessary. A tiered approach to severity levels enables swift prioritization and allocation of resources to address high-risk incidents promptly, minimizing potential impact on Box Manufacturing's operations.

Scope of Impact: The extent of the breach's impact on Box Manufacturing's network, systems, and data will influence the scale and complexity of the response effort. A comprehensive assessment of the scope of impact guides decision-making and resource allocation, enabling a proportionate and effective response to mitigate further damage and restore normal operations.

Communication Channels: Disruption of communication channels, such as email or phone services, may hinder the ability to coordinate response efforts and escalate incidents effectively. Contingency plans for alternative communication channels ensure uninterrupted communication and facilitate timely coordination and escalation of response activities, mitigating potential delays in incident resolution.

Incident Response Team Availability: The availability of key personnel, including Misha, Minka, and Cat, will impact the timeliness and effectiveness of the response, necessitating contingency plans for staffing shortages. Cross-training and succession planning ensure continuity of incident response operations, even in the absence of key personnel, maintaining resilience in the face of staffing challenges.

Email Template:

Communication to the Client (Percy F.):

Subject: Incident Response Notification

Dear Percy, Misha, and Minka,

I trust this email finds you well. Unfortunately, we have encountered a concerning security incident within Box Manufacturing's network that requires immediate attention. Here are the details:

Incident Description:

On March 28, 2024, at 2:30 PM AST, our security systems detected a sophisticated social engineering attack targeting Misha, the shift and production manager. Misha received a carefully crafted email containing a malicious attachment disguised as an urgent production report. Upon opening the attachment, malware was installed on Misha's computer, potentially compromising sensitive production data, including proprietary box designs and production schedules.

Immediate Action Taken:

1. Misha's computer has been isolated from the network to prevent further data exposure.

2. Our security team is conducting a thorough investigation to determine the extent of the breach and mitigate any potential damage.

3. All employees are being notified to remain vigilant and refrain from opening any suspicious emails or attachments.

Next Steps:

1. Our team will work diligently to remove the malware from Misha's computer and restore it to a secure state.

2. We will review and enhance our security protocols and conduct additional training sessions to reinforce security awareness among all employees.

3. We will keep you updated on the progress of our investigation and any additional measures taken to prevent similar incidents in the future.

Your cooperation and support during this challenging time are greatly appreciated. Please do not hesitate to reach out if you have any questions or concerns.

Best regards,
Madhuri Chamarthi
Incident Response Specialist

Communication to the Third-Party Provider (Cat):

Subject: **Urgent**: Security Incident Notification - Immediate Action Required

Dear Cat,

I hope this email finds you well. We are reaching out to inform you of a critical security incident that has occurred within Box Manufacturing's network and requires your immediate attention. Here are the details:

Incident Description:

On March 28, 2024, at 2:30 PM AST, we detected a sophisticated social engineering attack targeting Misha, the shift and production manager at Box Manufacturing. Misha received a malicious email attachment disguised as an urgent production report. Upon opening the attachment, malware was installed on Misha's computer, potentially compromising sensitive production data, including proprietary box designs and production schedules.

Immediate Action Taken:

1. Misha's computer has been isolated from the network to prevent further data exposure.

2. Our security team is conducting a comprehensive investigation to assess the scope of the breach and mitigate any potential damage.

3. Additional security measures are being implemented to prevent similar incidents in the future, including enhanced email security protocols and employee training sessions.

Next Steps:

1. We require your expertise to assist in analyzing the malware and identifying any additional security vulnerabilities within our network.

2. Your guidance on remediation strategies and best practices for enhancing our security posture would be invaluable in this situation.

3. We will keep you updated on the progress of our investigation and any actions taken to address the incident.

Your prompt attention and support are crucial as we work to resolve this security incident. Please let us know how you can assist us further.

Best regards,

Madhuri Chamarthi
Incident Response Specialist

Flowchart:

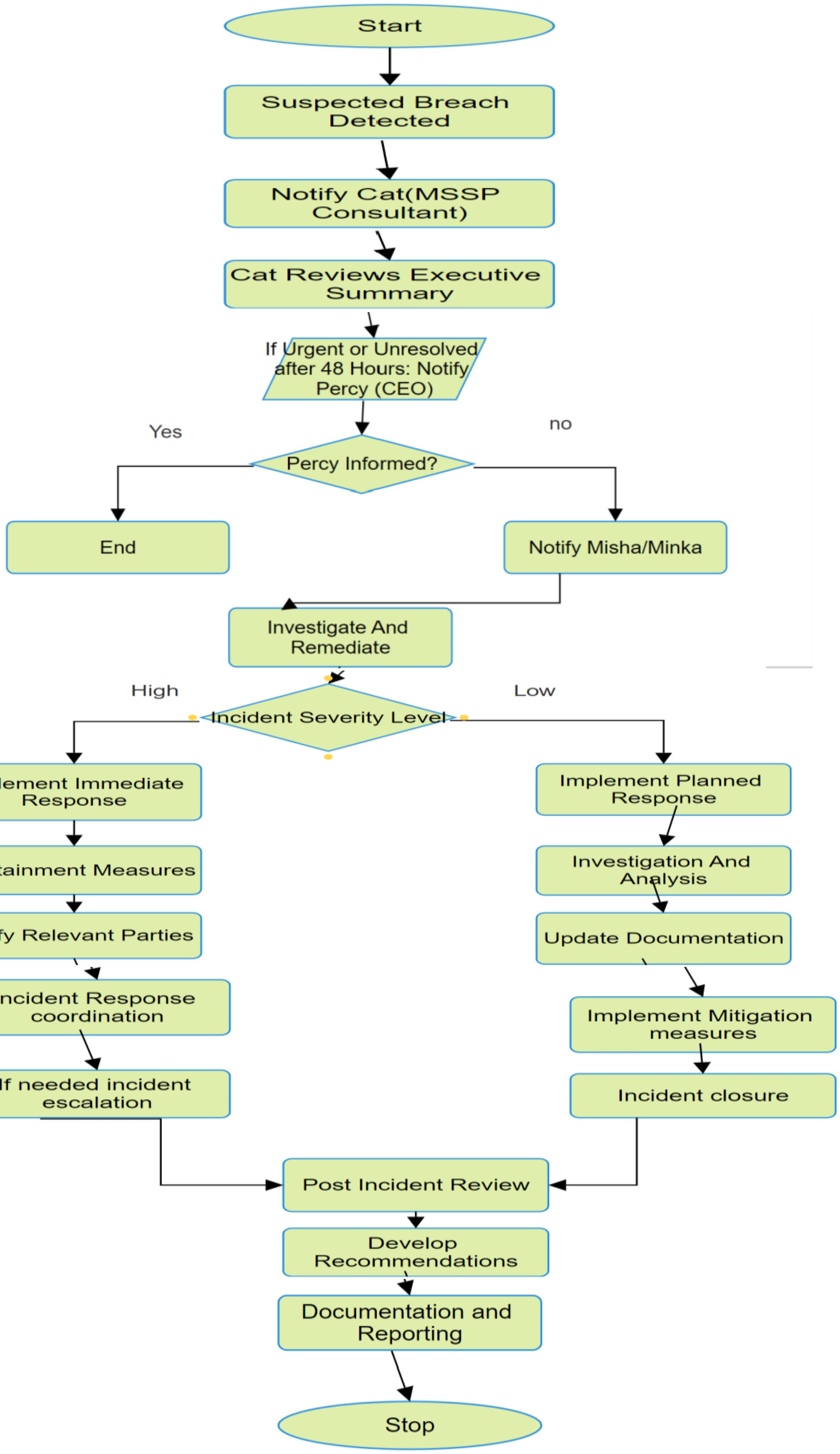
Start
Suspected Breach Detected
Notify Cat(MSSP Consultant)
Cat Reviews Executive Summary
If Urgent or Unresolved after 48 Hours: Notify Percy (CEO)
Yes
no
Percy Informed?
End
Notify Misha/Minka
Investigate And Remediate
High
Low
Incident Severity Level
Implement Immediate Response
Containment Measures
Notify Relevant Parties
Incident Response coordination
If needed incident escalation
Implement Planned Response
Investigation And Analysis
Update Documentation
Implement Mitigation measures
Incident closure
Post Incident Review
Develop Recommendations
Documentation and Reporting
Stop

Fig: Flowchart Representation of the incident

References:

How to Create an Incident Response Playbook- https://www.linkedin.com/pulse/how-create-incident-response-playbook-today-cybersecurity and

https://www.atlassian.com/incident-management/incident-response/how-to-create-an-incident-response-playbook#incident-response-lifecycle

Incident Response playbooks - https://learn.microsoft.com/en-us/security/operations/incident-response-playbooks

A brief Guide on Phishing, Incident Response &SOC -https://www.linkedin.com/pulse/brief-guide-phishing-incident-response-soc-start-ups-arunachalam

OpenAI. (n.d.). ChatGPT]. Retrieved from- https://openai.com/chatgpt

Federal Government Cybersecurity Incident and Vulnerability Response Playbook- Federal Government Cybersecurity Incident & Vulnerability Response Playbooks (cisa.gov)

Phases of Incident Response Plan- https://www.securitymetrics.com/blog/6-phases-incident-response-plan-