**Incident Response Playbook for Phishing Incident at Box Manufacturing**

By James Kuzhilaparambil

Contents

[1. Introduction 3](#_heading=h.gjdgxs)

[2. Executive Summary 3](#_heading=h.30j0zll)

[3. Key Roles and Responsibilities 3](#_heading=h.1fob9te)

[4. Playbook Steps 5](#_heading=h.3znysh7)

* + Detection and Reporting
  + Initial Analysis and Triage
  + Notification
  + Containment
  + Detailed Analysis and Reporting
  + Eradication and Recovery
  + Legal and Compliance
  + Communication
  + Post-Incident Review

[5. Rationale for Escalation 7](#_heading=h.2et92p0)

[6. Contact Information 7](#_heading=h.tyjcwt)

[7. Full Phishing Incident Report for Third-Party Provider (Cat) 8](#_heading=h.3dy6vkm)

[8. References 10](#_heading=h.1t3h5sf)

## 1. Introduction

**Purpose:** This playbook outlines the procedures for responding to cybersecurity incidents, specifically phishing attacks, for Box Manufacturing.  
**Scope:** Covers detection, analysis, containment, eradication, recovery, and post-incident review.

## 2. Executive Summary

On 1/1/2024, a phishing email was reported by an employee at Box Manufacturing. Initial analysis by the IT Security Team confirmed that the email was indeed a phishing attempt, potentially compromising systems and accounts. Immediate containment measures were implemented to prevent the spread of the threat. These measures included isolating affected systems, enhancing email filtering to block similar phishing attempts, and notifying relevant stakeholders.

Given the potential impact on critical systems and the risk of data compromise, it was deemed necessary to escalate the incident to our third-party provider, Cat. The decision to involve Cat was influenced by several factors, including the complexity of the threat, the need for specialized expertise in detailed analysis, and the requirement for comprehensive remediation strategies. Cat will provide a detailed analysis and full report, assessing the extent of the breach, recommending steps to eradicate the threat, and suggesting measures to prevent future incidents.

We will follow Cat’s recommendations to restore affected systems and services. We will keep you informed of any significant updates. If you have any questions or need further information, please do not hesitate to contact us.

## 3. Key Roles and Responsibilities

**Incident Response Manager (IRM)**

**Trigger:** Detection of a phishing email reported by an employee or automated systems.  
**Responsibilities:** Oversee the incident response process, coordinate with all teams, and ensure timely communication with the client and third-party provider.

**IT Security Team**

**Trigger:** Notification from the IRM or automated detection systems.  
**Responsibilities:** Analyze the phishing email, identify affected systems, and implement containment measures.

**Third-Party Provider (Cat)**

**Trigger:** Notification from the IRM about the suspected breach.  
**Responsibilities:** Conduct detailed analysis, provide a full report, and recommend actionable items.

**IT Support Team (Lucky)**

**Trigger:** Request from the IT Security Team or third-party provider for technical assistance.  
**Responsibilities:** Assist in isolating affected systems, restoring services, and applying security patches.

**Database Specialist (Dusty)**

**Trigger:** Involvement of database-related issues in the phishing incident.  
**Responsibilities:** Ensure the integrity and security of databases, assist in recovery if needed.

**Network Administrator (Ned)**

**Trigger:** Network-related issues detected during the incident.  
**Responsibilities:** Manage network security, isolate affected network segments, and assist in recovery.

**Legal Team**

**Trigger:** Potential legal implications or data breaches involving sensitive information.  
**Responsibilities:** Provide legal advice, ensure compliance with regulations, and handle any legal notifications.

**Public Relations (PR) Team**

**Trigger:** Need for public communication or media inquiries.  
**Responsibilities:** Manage external communication, prepare press releases, and handle media relations.

**Human Resources (HR)**

**Trigger:** Involvement of employees in the phishing incident.  
**Responsibilities:** Communicate with affected employees, provide training, and manage any disciplinary actions if necessary.

**Miss Misha F. (Shift and Production Manager)**

**Trigger:** Notification of major highlights and potential impacts from the IRM.  
**Responsibilities:** Stay informed about the incident’s impact on production and operations.

**Minka F. (Alternate Shift and Production Manager)**

**Trigger:** After-hours and weekend coverage for Miss Misha F.  
**Responsibilities:** Same as Miss Misha F. during her absence.

**Percy F. (CEO)**

**Trigger:** Escalated or urgent items, or unresolved issues after 48 hours.  
**Responsibilities:** Make executive decisions for escalated or unresolved issues based on the incident’s impact on the business.

## 4. Playbook Steps

Detection and Reporting

* **Employee reports a suspicious email to the IT Security Team.**
  + **Questions:**
    - When did you receive the email?
    - Did you click on any links or download attachments?
    - Have you noticed any unusual activity on your system?

Initial Analysis and Triage

* **IT Security Team analyzes the email to confirm it is a phishing attempt.**
  + **Questions:**
    - What is the source of the email?
    - Are there any known indicators of compromise (IOCs)?
    - Which systems or accounts might be affected?

Notification

* **IRM notifies Miss Misha F. (or Minka F. after hours) about major highlights and potential impacts.**
* **IRM notifies Cat (Third-Party Provider) about the suspected breach.**
  + **Questions:**
    - What is the initial assessment of the incident?
    - What information needs to be shared with the third-party provider?

Containment

* **IT Security Team implements containment measures to prevent the spread.**
  + **Questions:**
    - Which systems need to be isolated?
    - What immediate actions are required to contain the threat?
    - Are there any ongoing threats that need monitoring?

Detailed Analysis and Reporting

* **Cat conducts a detailed analysis and prepares a full report with actionable items.**
  + **Questions:**
    - What is the extent of the breach?
    - What are the recommended steps to eradicate the threat?
    - What measures should be taken to prevent future incidents?

Eradication and Recovery

* **IT Support Team (Lucky) assists in eradicating the threat and restoring systems based on Cat’s recommendations.**
* **Database Specialist (Dusty) ensures database integrity and assists in recovery if needed.**
* **Network Administrator (Ned) manages network security and assists in recovery.**
  + **Questions:**
    - What steps are needed to remove the phishing threat?
    - How will we ensure the systems are secure before bringing them back online?
    - What recovery measures are in place to restore normal operations?

Legal and Compliance

* **Legal Team assesses any legal implications and ensures compliance.**
  + **Questions:**
    - Are there any data breaches involving sensitive information?
    - What regulatory requirements must we comply with?
    - Do we need to notify any external parties or authorities?

Communication

* **PR Team manages external communication and media relations.**
  + **Questions:**
    - What information needs to be communicated to the public?
    - How will we handle media inquiries?
    - What is our messaging strategy to maintain trust and transparency?

Post-Incident Review

* **All teams conduct a post-incident review to identify lessons learned.**
  + **Questions:**
    - What worked well in our response?
    - What areas need improvement?
    - How can we update our policies and procedures to prevent future incidents?

## 5. Rationale for Escalation

The decision to escalate incidents and involve additional resources or individuals is influenced by several critical factors:

* **Complexity of the Threat:** When the phishing attempt involves sophisticated techniques that require specialized expertise beyond our in-house capabilities.
* **Potential Impact:** If the incident has the potential to compromise critical systems and sensitive data, necessitating a thorough and expert analysis.
* **Need for Comprehensive Remediation:** When the potential scope of the breach requires additional resources to ensure a comprehensive and effective remediation strategy.
* **Specialized Expertise:** Involving third-party providers like Cat, who possess the necessary skills and experience to conduct detailed analysis and provide actionable recommendations to mitigate the threat and prevent future incidents.

## 6. Contact Information

* **Percy F. (CEO):** percy@box.cat
* **Miss Misha F. (Shift and Production Manager):** mesha@box.cat, Phone 902-9836
* **Minka F. (Alternate Shift and Production Manager):** minka@box.cat, Phone 562-7658
* **Dusty (Database Specialist):** dusty@box.cat, Phone 462-8952
* **Lucky (IT Support Specialist):** lucky@box.cat, Phone 269-5466
* **Ned (Network Administrator):** ned@box.cat, Phone 877-4332
* **Cat (Third-Party Provider):** cat@soc.cat, Phone 905-4616 or cell 902-4321
* **Incident Response Manager (IRM):** alex.p@infosecurity.com, Phone 905-237-3478
* **IT Security Team:** itsec@infosecurity.com, Phone 905-648-3458
* **Legal Team:** legal@box.cat, Phone 810-9960
* **Public Relations (PR) Team:** pr@box.cat, Phone 896-5012
* **Human Resources (HR):** hr@box.cat, Phone 866-4032

## 7. Full Phishing Incident Report for Third-Party Provider (Cat)

**Incident Summary:**

* Date and Time: 1/1/2024
* Description: A phishing email was reported by an employee. Initial analysis confirms it is a phishing attempt.
* Impact: Potential compromise of systems and accounts.

**Initial Analysis:**

* **Source of Email:** [**phishing@example.com**](mailto:phishing@example.com)

The phishing email originated from an external email address, phishing@example.com, which is not associated with any known contacts or legitimate businesses. The email header analysis revealed that the email was sent from an IP address located in a region known for cybercriminal activity. The email contained a spoofed sender address, making it appear as if it was sent from a trusted internal source.

* **Indicators of Compromise (IOCs):**

Email Subject: “Urgent: Action Required for Your Account”

Malicious Links: The email contained a link to http://malicious-site.com/login, which is a known phishing site.

Attachment: The email included an attachment named Invoice.pdf that, when opened, attempts to download malware.

Suspicious Domains: The email referenced domains such as malicious-site.com and fake-login.com.

IP Address: The email was sent from IP address 192.168.1.100, which has been flagged in threat intelligence databases.

* **Affected Systems/Accounts:**

 Employee Accounts: The email was sent to multiple employees, including employee1@box.cat and employee2@box.cat.

User Workstations: The workstations of the employees who received the email may be compromised if they clicked on the link or opened the attachment.

Email Server: The email server may need to be checked for any signs of compromise or additional phishing emails.

Network Segments: The network segments where the affected workstations are located should be monitored for any unusual activity.

**Actions Taken:**

* **Initial Response:** The IT Security Team has analyzed the email and confirmed it as a phishing attempt.
* **Containment Measures:**
  + Isolated affected systems.
  + Implemented email filtering to block similar phishing attempts.
  + Notified relevant stakeholders.

**Rationale for Escalation:** The decision to escalate this incident to our third-party provider, Cat, was influenced by several critical factors:

* **Complexity of the Threat:** The phishing attempt involved sophisticated techniques that required specialized expertise beyond our in-house capabilities.
* **Potential Impact:** The incident had the potential to compromise critical systems and sensitive data, necessitating a thorough and expert analysis.
* **Need for Comprehensive Remediation:** Given the potential scope of the breach, it was essential to involve additional resources to ensure a comprehensive and effective remediation strategy.
* **Specialized Expertise:** Cat possesses the necessary skills and experience to conduct a detailed analysis and provide actionable recommendations to mitigate the threat and prevent future incidents.

**Request for Detailed Analysis:** We request you to conduct a detailed analysis of the incident and provide a full report with actionable items. Please include the following in your report:

* **Extent of the Breach:** Detailed assessment of the scope and impact.
* **Recommended Steps to Eradicate the Threat:** Specific actions to remove the phishing threat.
* **Measures to Prevent Future Incidents:** Recommendations for improving security measures to prevent similar incidents.

**Next Steps:**

* **Third-Party Analysis:** Awaiting detailed analysis and recommendations from Cat.
* **Recovery Plan:** Implementing recovery measures based on Cat’s recommendations.

**Contact Information:**

* **Incident Response Manager:** Alex P., alex.p @infosecurity.com, (905)237 3478
* **IT Security Team:** admin, itsec@infosecurity.com, (905)648 3458

Please prioritize this request and provide your report at the earliest convenience.

Best regards,

Alex P.  
Incident Response Manager  
Box Manufacturing

## 8. References

1. Cichonski, P., Millar, T., Grance, T., Scarfone, K., National Institute of Standards and Technology, United States Computer Emergency Readiness Team, & Scarfone Cybersecurity. (2012). *Computer security incident handling guide* (NIST Special Publication 800-61, Revision 2). https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf
2. Phishing | Incident Response Playbooks Gallery. (n.d.). https://incidentresponse.org/playbooks/phishing
3. Exabeam. (2024, June 12). *Incident response playbook: 6 key elements, examples, and tips for success*. https://www.exabeam.com/explainers/information-security/incident-response-playbook-6-key-elements-examples-and-tips-for-success/
4. Cybersecurity and Infrastructure Security Agency. (2021). *Cybersecurity incident & vulnerability response playbooks*. https://www.cisa.gov/sites/default/files/2024-08/Federal\_Government\_Cybersecurity\_Incident\_and\_Vulnerability\_Response\_Playbooks\_508C.pdf
5. MITRE ATT&CK Framework. (n.d.). *MITRE ATT&CK*. https://attack.mitre.org/
6. National Institute of Standards and Technology. (2020). *NIST cybersecurity framework*. https://www.nist.gov/cyberframework
7. SANS Institute. (2023). *Incident handler’s handbook*. https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901
8. Symantec. (2023). *Phishing attack trends*. https://www.symantec.com/security-center/threat-report
9. Verizon. (2023). *Data breach investigations report*. https://www.verizon.com/business/resources/reports/dbir/
10. Ponemon Institute. (2023). *Cost of a data breach report*. https://www.ibm.com/security/data-breach
11. Microsoft. (2023). *Microsoft security intelligence report*. https://www.microsoft.com/security/blog/microsoft-security-intelligence-report/
12. FireEye. (2023). *M-Trends 2023: Threat report*. https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html
13. Cisco. (2023). *Cisco 2023 annual cybersecurity report*. https://www.cisco.com/c/en/us/products/security/security-reports.html
14. Palo Alto Networks. (2023). *Unit 42 incident response report*. https://unit42.paloaltonetworks.com/incident-response-report/
15. CrowdStrike. (2023). *Global threat report*. https://www.crowdstrike.com/global-threat-report/