**PROJECT 4**

**Title: Incident Response Playbook for Cat and Box**

***By Titobiloluwa (Tito) Ilori***

**Table of Content**

|  | **Sections** | **Page No.** | |
| --- | --- | --- | --- |
| **1** | **Introduction to the Incidence Response Playbook** | | **2** |
| **2** | **Box Manufacturing Company Playbook** | | **3** |
| **3** | **A List of Top Incidences and Trigger Items That May Affect The Flow** | | **6** |
| **4** | **A Sample or Letter Template to the Client** | | **7** |
| **5** | **A Sample or Letter Template to the Third-Party Provider** | | **8** |
| **A** | **Incidence Response Lifecycle Explained** | | **9** |
| **B** | **Reference** | | **12** |

1. **INTRODUCTION TO THE INCIDENT RESPONSE PLAYBOOK**

Playbooks are **SOPs** (Standard Operating Procedures) used by cybersecurity specialists or the SOC (Security Operation Centre) for cyber-related incidents. It provides “a standardized response process for cybersecurity incidents and describes the process and completion through the incident response phases as defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61 Rev. 2,1 including preparation, detection and analysis, containment, eradication and recovery, and post-incident activities.”2

A diagram of a life cycle

Description automatically generated

Fig 1: NIST Incident Response Plan/Lifecycle indicating the phases.3

1. **BOX MANUFACTURING COMPANY PLAYBOOK**

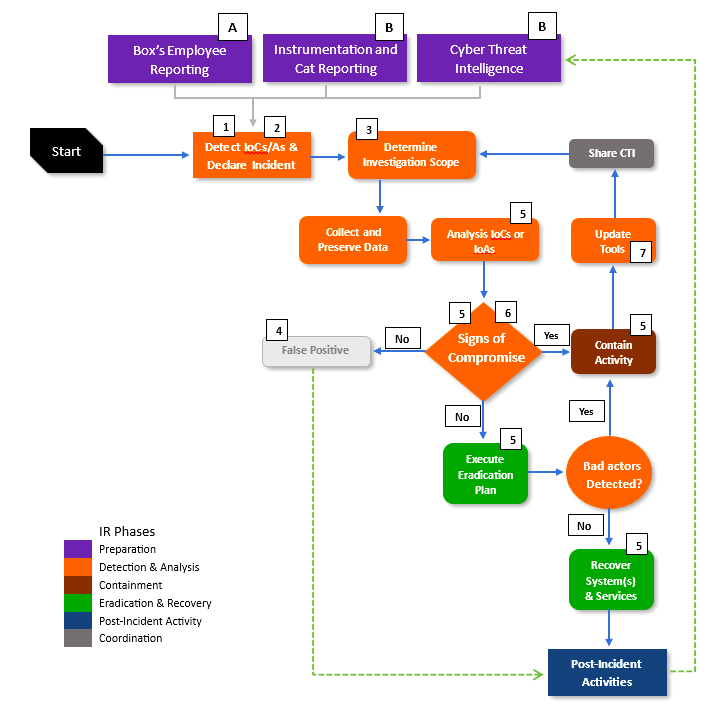
**PREPARATION PHASE:**

1. Policies and procedures about notification, interaction, and information.
   * Cat is the Cybersecurity who oversees all of Box’s cybersecurity needs.
   * Cat communicates important cybersecurity decisions with all parties (CEO and employees) as necessary.
   * Cat is a go-to for every cybersecurity need within the company based on his contract. She is a Managed Security Service Provider to the company. She has provided a daytime phone number, as well as an after-hours and weekend cell number.
   * The primary contact for cybersecurity incidents from the client is SOC. Cat also contacts or declares the incident to the SOC – the incident response team to further perform detection, analysis, containing, eradication, and recovery.
   * The CEO (Percy) should be informed personally if an item is escalated or urgent, or unresolved after 48 hours.
   * Cat will inform the Shift and Production Managers of any potential impact and any major highlights (from user reports or telemetry/infrastructure monitoring) caused by any breach of the system: (Misha) works 9 AM to 5 PM AST weekdays, but has an alternate, Minka F. covers for her after-work hours and during weekends.
2. Instrumentation and CTI
   * Cat performs telemetry to support the system and sensor-based detection and monitoring capabilities to alert her when there is a suspected breach into the security posture of the company.
   * Also, the use or adaptation of Cyber Threat Intelligence to identify known malicious behaviour.

| **Parties** | **Position/Role** | | **Name** | **Email Address** | **Phone** |
| --- | --- | --- | --- | --- | --- |
| **BOX Manufactrng** | ***Chief Exec. Officer*** | | Mr Percy F | percy@box.cat |  |
| ***Shift & Production Managers*** | *9AM – 5PM Weekdays* | Miss Misha F. | mesha@box.cat | 902 66-9999 |
| *After Hours* | Minka F. | minka@box.cat | 902 99-9999 |
| **3rd Party** | ***MSSP*** | | Consultant Cat | cat@soc.cat | 902 88-1234  cell 902 77-4321 |
| ***Security Operation Centre*** | | SOC |

***Tab 1: Parties' roles and contact information.***

My recommendation is that the Client, Cat and SOC follow the industry standard briefly described earlier in the NIST Incident Response Playbook (NIST Special Publication 800-61) above. Below is the summarized and recommended flowchart for Box Manufacturing Company.



***Fig 2: Playbook flowchart (Numbered) indicating instructions for Box’s Users or Shift Production Managers, Cat, and SOC.***

**NUMBER KEY EXPLAINED:**

**1.** Incident immediately reported by Misha or Minka, either during Work or after work to SOC and Copy Cat.

**2.** Cat detects anomalous/malicious behaviour from instrumentation or CTI and declares the incident to SOC for Incident Response playbook activation and informs the Shift and Production Managers (SPMs) immediately, either during work (Misha) or after Work hours (Minka).

**3.** If IoC (Indicator of Compromise) or IoA (Indicator of Attack) causes a high impact on either or all the CIA triad, escalate as urgent and inform the CEO.

**4.** If there are no signs of compromise and the event reported was not malicious (for instance, the CEO or authorized user logged in with Admin Privilege without prior communication with Cat or SPMs in odd hours and it triggers), pass the phase to post-incident and recommended proper communication to avoid alert fatigue.

**5.** Any incident within 48 hours from detection and declaration till containment or eradication or recovery should not be reported to the CEO, only the Cat and SPMs. Otherwise (48 hours or more), the CEO must be informed.

**6.** SOC determines the escalation or priority of the attack (using CIA triad, CVSS or CTI), and informs the CEO and any related law enforcement agency.

**7.** Update the detection tools’ configuration in case of a Zero-day attack.

For a further breakdown of each phase in the Incidence Response lifecycle, please read through the section in Appendix A.

**3. A LIST OF TOP INCIDENCES AND TRIGGER ITEMS THAT MAY AFFECT THE FLOW**

In the next section, I will mention three (3) incidents that are common to small businesses which I will recommend this playbook for. I will briefly discuss the relevance of adopting this playbook to maintain industry security posture.

1. **Phishing Attack:** According to Forbes.com, Phishing is one of the most prevalent types of cybercrimes with over 500 million phishing attacks reported in 2022. There were 300,497 phishing victims with a total loss of $52,089,159 in the U.S. alone.4 Knowing that this vulnerability is very common, it is important to set up a playbook that mitigates or controls this incident if it occurs.
2. **Data Breach/Theft:** This means when data is being extracted by external or internal parties. The most common types of attacks on small businesses include Phishing/Social Engineering (57%), Compromised/Stolen Devices (33%) and Credential Theft (30%).5 As a small manufacturing company, this is important as well, to protect customers' PII, credit card information, company’s intellectual property.
3. **Distributed Denial of Service:** According to TechInsurance.com, a distributed denial-of-service (DDoS) attack overwhelms its target with a flood of traffic from malware-infected devices. It maxes out the capacity of the target host and blocks normal traffic to the host with a denial-of-service error. Small to medium-sized businesses (SMBs) spend an average of US$120,000 restoring service and managing operations during a DDoS attack.6

**A list of trigger items that may affect the flow:**

These are a few cyber-incidences with high priority and high impact on the Confidentiality, integrity, and availability of the company’s assets (people, information/data, devices and technology) and should be escalated and treated as urgent.

* **Authorized access** = Internal or external user gains access to the network illegally.
* **Malware or Virus Outbreak** = Malware detected running rampant on the network and causing a breach of the company’s data or intellectual property.
* **Distributed Denial of Service** = System performance or availability is compromised.
* **Root access** = Unauthorized root/admin access has been detected.
* **Insider threat or elevation of privilege**: User of system credentials have been compromised.
* **Backdoor or remote access Command and Control detected**.

1. **A SAMPLE OR LETTER TEMPLATE TO THE CLIENT**

This is the sample/letter template as a response to the incident report received from the client.

**Dear Client**

This is a response to the incident report received on \_\_\_\_\_\_\_\_\_\_\_\_\_ (Date and time).

We want to assure you that we immediately started looking into the incident as submitted.

Here is the contact of two members of our team (work hours or after-work hours) that will reach out to you or the affected user(s). You can as well call or send emails to the email addresses provided.

Work hours: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

After-Work hours: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

According to standard procedure, this is the timeline required to recover this incident: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Listed here are the recovery actions:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Here are the lessons learnt to prevent similar issues in the future:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

For your information, this is the summary of the actions taken and the final outcome of the resolution:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Finally, we will love to advise and remind you that sensitive information about your company and your customers must be handled securely always and only share with authorized personnel on a need-to-know basis.

Sincerely,

- name -

- designation -

SOC Team

**5. A SAMPLE OR LETTER TEMPLATE TO THE THIRD-PARTY PROVIDER**

*This is a letter template that the Shift and Production Managers will send to inform or report to Cat (the Managed Security Service Provider) and Security Operation Centre (SOC) of occurring cyber incidents in the company.*

**Dear SOC**

I am writing this letter to inform you about an event/incident that has occurred within our systems.

This incident was first noticed: \_\_\_\_\_\_\_\_\_\_\_ (specify date and time).

Brief description of the issue or incident:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

List of affected systems or services: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Initial action taken: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Contact Information of the user(s) reporting the incident for further investigation: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The evidence of unusual behaviour or error messages displayed (any other relevant information) is: \_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

The potential impact of this incident is/are: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

I have cc’d Cat in this report. We look forward to a timely response to this incident report as an optimum security posture of our company is critical to its production and reputation in the industry.

Best regards

- Name -

Shift and Production Manager

Box Manufacturing Company.

**APPENDIX A: INCIDENT RESPONSE LIFECYCLE EXPLAINED**

In the next section, I will highlight the key components of the incident response playbook (as described in Cybersecurity Incident & Vulnerability Response Playbooks by CISA)2, then specialise on a few specific cyber-incidences that this workflow/playbook can be used for. A diagram of a process flow

Description automatically generated

***Fig 3: Incident Response Process by CISA2***

1. **Preparation Phase**: This is to prepare for major incidents before they occur to mitigate any impact on the Box Organization.
   1. Policies and Procedures: This should include processes for designating incident managers and addressing notification, interaction, and evidence sharing with law enforcement.
   2. Instrumentation: maintain an accurate picture of infrastructure (systems, networks, cloud platforms, and contractor-hosted networks) by widely implementing telemetry to support system and sensor-based detection and monitoring capabilities.
   3. Leveraging Cyber Threat Intelligence: Cat should actively monitor intelligence feeds for threat or vulnerability advisories from the government, trusted partners, open sources, and commercial entities.
   4. Educate users on cyber threats and notification procedures.
   5. Operational Security (OPSEC): Ensure that IR and defensive systems and processes will be operational during an attack, particularly in the event of pervasive compromises—such as a ransomware attack.
2. **Detention and Analysis:** To detect and analyze events, implement defined processes, appropriate technology, and sufficient baseline information to monitor, detect, and alert on anomalous and suspicious activity.
   1. Declare Incident: Declare an incident by reporting it to CISA at <https://www.us-cert.cisa.gov/> and alerting agency IT leadership to the need for investigation and response.
   2. Determine Investigation Scope: Use available data to identify the type of access, the extent to which assets have been affected, the level of privilege attained by the adversary, and the operational or informational impact.
   3. Collect and Preserve Data: Collect and preserve data for incident verification, categorization, prioritization, mitigation, reporting, and attribution.
   4. Perform Technical Analysis: Correlate information, assess anomalous activity against a known baseline to determine the root cause, and document adversary TTPs (Tactics, Techniques and Procedures) to enable prioritization of the subsequent response activities.
   5. Correlate Events and Document Timeline
   6. Identify Anomalous Activity
   7. Identify Root Cause and Enabling Conditions
   8. Gather Incident Indicators
   9. Analyze for Common Adversary TTPs
   10. Validate and Refine Investigation Scope
3. **Containment**: The objective is to prevent further damage and reduce the immediate impact of the incident by removing the adversary’s access. Summarized Containment activities below.
   1. Isolate impacted systems and network segments from each other and/or from impacted systems and networks.
   2. Capture forensic images to preserve evidence for legal use or further investigation.
   3. Update firewall filtering
   4. Block malware sources and close specific ports and/or mail servers or relevant services.
   5. Redirect the adversary to a sandbox (a form of containment)
   6. Change admin credentials, rotate private keys etc.
4. **Eradication & Recovery**: to allow the return of normal operations by eliminating artefacts of the incident (e.g., remove malicious code, re-image infected systems) and mitigating the vulnerabilities or other conditions that were exploited.
   1. ***Execute Eradication Plan***
      1. Remediating all infected IT environments
      2. Reimaging affected systems, and rebuilding systems from scratch.
      3. Rebuilding hardware (required when the incident involves rootkits).
      4. Replacing compromised files with clean versions.
      5. Installing patches.
      6. Resetting passwords on compromised accounts.
      7. Allow adequate time to ensure all systems are clear of all possible threat actor persistence mechanisms (backdoors, etc.) as adversaries often use more than one mechanism.
   2. Recover System(s) and Services
      1. Reconnecting rebuilt/new systems to networks.
      2. Tightening perimeter security and zero trust access rules.
      3. Testing systems thoroughly, including security controls.
      4. Monitoring operations for abnormal behaviours.
5. **Post-Incident Activities**: Document the incident, inform agency leadership, harden the environment to prevent similar incidents, and apply lessons learned to improve the handling of future incidents.
   1. ***Adjust Sensors, Alerts, and Log Collection***
   2. ***Finalize Reports***
   3. ***Perform Hotwash*** (a lessons-learned analysis to review the effectiveness and efficiency of incident handling.)
6. **Coordination:** This is coordination by a federal body or agency, e.g. CISA. Some agencies have special authorities, expertise, and information that are extremely beneficial during an incident.

**APPENDIX B: REFERENCE**

1. NIST Special Publication (SP) 800-61 Rev. 2: Computer Security Incident Handling Guide - Paul Cichonski, et al (August 2012) <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>
2. Cybersecurity Incident & Vulnerability Response Playbooks - CISA (November 2021) - <https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf>
3. NIST Incident Response Plan: Steps and Template - DAN DURAN (July 7, 2022) <https://rhyno.io/nist-incident-response-plan-steps-and-template/>
4. Phishing Statistics By State In 2023 - Kelly Mai & Cassie Bottorff (June 9, 2023) <https://www.forbes.com/advisor/business/phishing-statistics/>
5. 2023 Must-Know Cyber Attack Statistics and Trends Mike Mclean (June 1, 2023) - <https://www.embroker.com/blog/cyber-attack-statistics/>
6. How much will a DDoS attack cost your small business? (April 7, 2022) - <https://www.techinsurance.com/resources/ddos-small-business-costs>