

# Mobile Security Incident Response Playbook

<b>Title</b>	Mobile Security Incident Response Playbook
<b>Version</b>	V1
<b>Date issued</b>	DD-MM-YYYY
<b>Status</b>	In progress
<b>Document owner</b>	Full Name
<b>Creator name</b>	Full Name
<b>Creator organization name</b>	<Organization Name>
<b>Subject category</b>	Mobile Security Incident Response
<b>Access constraints</b>	NA
<b>Review cycle</b>	Annually

## 1. Introduction

### 1.1. Incident Overview

Mobile-based security incidents have become increasingly common owing to the implementation of BYOD/COBO policies across various organizations. Attackers target mobile devices used for business purposes in and out of organizations with the intention of gaining access to critical corporate data or perform other malicious activities.

Assume that a few employees of organization Z are suspected to be involved in the installation of a malicious application on the company's Android mobile devices. The malicious application can potentially compromise the entire company's network. This playbook describes different activities related to various stages of incident response for better implementation of incident response procedures in case of mobile-based security incidents.

### 1.2 Purpose of Playbook

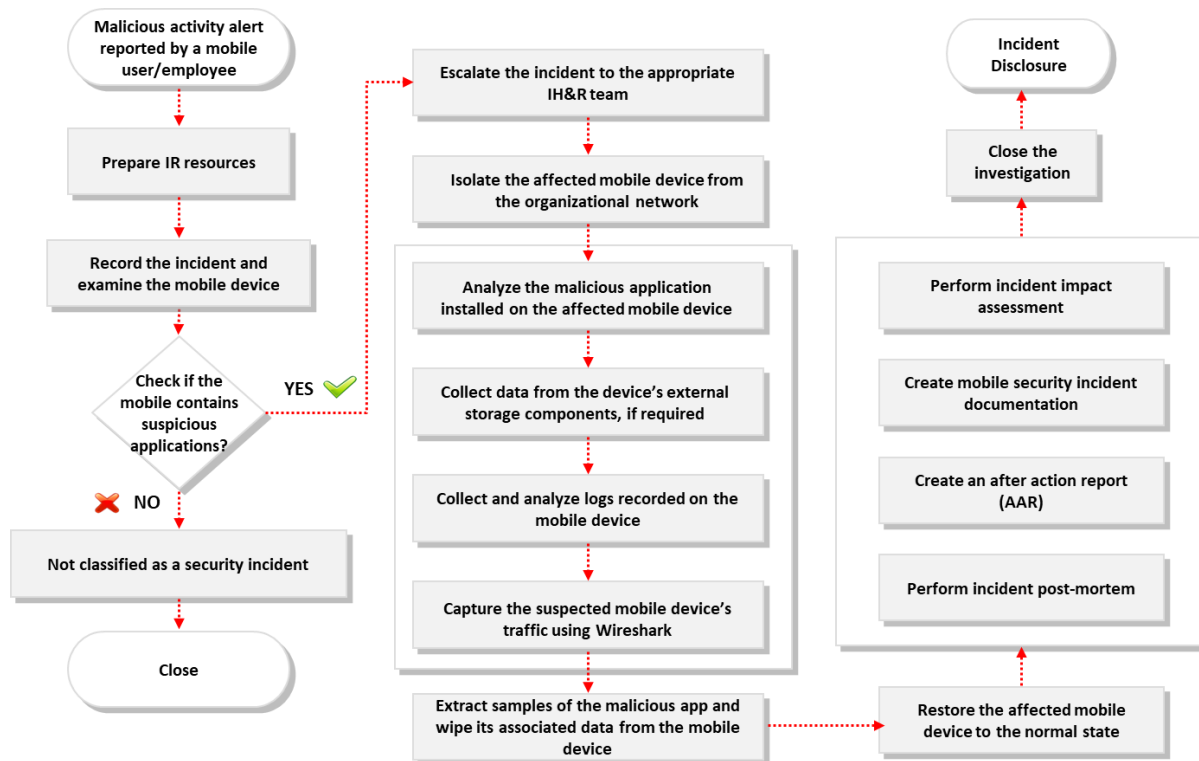
The main purpose of this playbook is to provide guidance for detecting and responding to mobile-based security incidents within an organization. This playbook includes step-wise guidance for the IH&R team to implement mitigative actions and defend against various Android-based mobile attacks in an organization.

### 1.3 Scope

This playbook is developed for the use of incident responders to handle mobile-based security incidents in an organization. Additionally, this document must be used alongside the incident response plan of the organization. The scope of this document is listed below (not limited to):

- Determine the total number of mobile devices on which the malicious application was installed
- Determine the risks involved with the malicious application installed on devices
- Determine the incident source
- Determine the damage caused by the incident
- Identify backdoor activities as well as command and control (C&C) server connections
- Analyze the infected mobile devices
- Recover from the incident

### 1.4 Workflow Diagram



Workflow diagram for mobile security incident response

## 2. Preparation

### 2.1 Objectives

The main objective of the preparation phase is to prepare the IH&R team to respond to mobile-based security incidents in an effective and timely manner. Another objective of this phase is to define the roles of employees, along with their reporting mechanisms, for mitigating a mobile security incident.

### 2.2 Activities Involved

*[Activities may differ based on organizational policies, but they are not limited to the following.]*

- Prepare for incident response:
  - Prepare, review, and practice the incident response procedures in accordance with the incident response plan
  - Implement security policies to prevent rooted mobile devices from accessing company resources
  - Perform cost benefit or budget analysis
  - Select a clean workstation to install the required mobile incident response tools
  - Design an accurate picture of assets deployed across different departments
  - Incorporate appropriate data loss prevention (DLP) and disaster recovery (DR) plans before beginning the investigation
  - Establish out-of-band communication between the IH&R teams and employees
  - Configure mobile device management (MDM) as well as identity and access management (IAM) solutions to detect various mobile-based security incidents at the earliest
  - Incorporate threat intelligence into the existing security capabilities to feed them with the latest risks, vulnerabilities, common patterns, etc.
  - Provide easy access to the required documentation such as incident response plan and network architecture to respond to a mobile security incident. Links of important documents are given below:
    - Reference 1:
    - Reference 2:
    - Reference 3:
  - Deploy mobile device monitoring tools such as Kandji and Citrix Endpoint Management to monitor mobile devices from a remote location within the organization

- Implement automation for mobile-based security and the IH&R process
- Identify devices, their operating systems, and other installed apps; then, correlate these data with mobile threat intelligence
- Configure security controls to provide alerts regarding mobile device usage patterns and behavior of the associated application
- Deploy mobile application management (MAM) solutions to manage employee devices
- Configure mobile data acquisition tools such as Cellebrite UFED and Oxygen Forensics to perform physical/logical data acquisition in a mobile device for further investigation
- Configure log analysis tools such as SolarWinds® Loggly® and LogRabbit to detect malicious activities in mobile devices
- Deploy Android malware analysis tools such as DeGuard and ClassyShark to analyze the malware and detect malicious activities performed on the device
- Configure reverse engineering tools such as Radare2 and Apktool to decode and analyze mobile applications
- Inform the employees:
  - Conduct regular training and awareness programs demonstrating mobile vulnerabilities, malicious applications, and other mobile security incidents
  - Create a proper format for reporting and registering complaints
  - Ensure that training and awareness sessions are mandatory for employees handling critical data and assets of the organization
  - Provide proper contact information of personnel who can be contacted by users in case of a mobile security incident

### 2.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Prepare for incident response ○ Create incident response processes and procedures	CISO	Email, Phone, Text Message
	Information Security Manager	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message

<ul style="list-style-type: none"> <li>○ Define roles and responsibilities</li> <li>○ Review recent incident reports</li> <li>○ Incorporate threat intelligence</li> <li>○ Maintain network architecture and data flow diagrams</li> <li>○ Define threat indicators and incorporate alerting solutions</li> </ul>	Service Desk	Email, Phone, Text Message
	Service Delivery Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Administrators	Email, Phone, Text Message
	Legal Team	Email, Phone, Text Message
	Federal Agency	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
<p>Inform the employees</p> <ul style="list-style-type: none"> <li>○ Conduct training and awareness sessions on mobile-based security incidents</li> </ul>	Information Security Manager	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	HR Manager/Director	Email, Phone, Text Message
	Administrators	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message

## 2.4 Additional Information (if any)

**Note:** Refer to the following templates and checklists to fill the necessary details:

- Preparation to Mobile-based Security Incidents Checklist.docx
- Mobile-based Security Incident Handling Toolkit.docx
- IH&R Plan Template.docx

### 3. Detection and Notification

#### 3.1 Objectives

The main objective of the detection phase involves performing initial investigation on the suspected mobile device and determine the activities of the installed malicious application.

#### 3.2 Activities Involved

*[Activities may differ based on organizational policies, but they are not limited to the following.]*

- Detect the mobile-based security incident through initial investigation
  - Check for popups or advertisements being displayed on the device
  - Check for unwanted applications running on the device
  - Check whether the device is consuming excessive mobile data
  - Check whether the mobile device's battery is depleting quickly
  - Check for strange voice or text messages
  - Check whether files or folders are saved with strange names
  - Check whether the device is running in the optimal state
  - Identify unwanted permissions given to the installed applications
  - Check whether the device is automatically rebooting
  - Check if the device is overheating
  - Check for unknown modifications in device settings
  - Check if the device is running on outdated operating system
  - Check if the device is connected to unsecured Wi-Fi networks
  - Check for signs of activity after keeping the device in a standby mode
  - Check if the device is consuming more time to shut down or restart
  - Check for unrecognized or fake icons on the device screen
  - Check for applications requesting permission to access other installed/building applications
  - Escalate the mobile security incident to higher authorities with the proper escalation procedure
- Gather the following information from initial investigation:
  - Type of incident
  - Location of the incident
  - Who, how, and when was the incident reported

- List of users/employees whose mobile devices were infected
- Gather complete information such as apps installed, operating system version, and type of device
- Identify the causes behind the incident
- Number of mobile devices affected
- Impact on business operations

### 3.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Detecting the incident <ul style="list-style-type: none"> <li>○ Monitor security solutions</li> <li>○ Respond to manual and automated alerts</li> <li>○ Escalate the incident via the ticketing system (if not escalated)</li> </ul>	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message
Initial investigation <ul style="list-style-type: none"> <li>○ Collect initial evidence data</li> <li>○ Classify and prioritize the incident</li> </ul>	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	Head of IT	Email, Phone, Text Message
Notification of the incident	Information Security Manager	Email, Phone, Text Message

○ Follow the defined IH&R plan to notify the incident	IH&R Team	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message

### 3.4 Additional Information (if any)

**Note:** Refer to the following documents to fill the necessary details:

- d. Mobile-based Security Incidents Detection and Analysis Template.docx
- e. Incident Identification and Validation Template.docx
- f. Incident Priority Template.docx
- g. Incident Communication Logs Template.docx
- h. Point-of-Contact Template.docx

## 4. Containment

### 4.1 Objectives

The main objective of the containment phase is to identify mobile devices affected by the malicious application and isolate them from the network.

### 4.2 Containment Steps/Activities

*[Activities may differ based on organizational policies, but they are not limited to the following.]*

- Activities to contain mobile-based security incidents:
  - Isolate the mobile device by disconnecting it from the organizational network and shutting it down only after acquiring evidence data
  - Reboot the mobile device into safe mode to isolate malicious applications
  - Reset the password of bank, email, social media, and other online accounts logged into through the device and use multifactor authentication
  - Run malware detection tools to identify the affected applications
  - Filter and block unusual login attempts or traffic directed toward the device's applications
  - Implement tools such as TotalAV Antivirus and Malwarebytes to delete any spyware installed on the device
  - Disable the wireless feature if not in use
  - Block VPN or other remote network access connections



- Remove or uninstall compromised/malicious applications
- Limit permissions to applications
- Disable unauthorized permissions granted to applications
- Install and enable Trend Micro Mobile Security's Wi-Fi Checker to get alerts related to unsecured wireless connections
- Utilize the remote wipe feature to remove critical data from the infected mobile devices
- Stop vulnerable services and block access to company resources
- Perform security checkups to fix security issues in the mobile device and user account
- Communicate the progress:
  - Regularly inform the stakeholders about the status of the incident handling process

### 4.3 Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Containment activities	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message

### 4.4 Additional Information (if any)

**Note:** Refer to the following documents to fill the necessary details:

- i. Containment of Mobile-based Security Incidents Checklist.docx
- j. Incident Containment Checklist.docx
- k. Incident Containment Template.docx

## 5. Analysis

### 5.1 Objectives

The main objective of this phase is to analyze the security incident and determine its scope. Another objective of this phase is to detect and report the incident impact to

establish forensic investigation requirements and develop an effective mitigation strategy based on analysis results.

## 5.2 Activities Involved

*[Activities may differ based on organizational policies, but they are not limited to the following.]*

- Analyze the scope of mobile security incident:
  - Perform log analysis on the Android device to determine the root cause of the incident
  - Use tools such as Flurry Analytics to analyze active accounts and sessions on the device
  - Collect data from other external storage components of the device such as SIM and SD cards for further investigation
  - Use packet-capturing tools such as PCAP Remote and Wireshark to capture and analyze network traffic originating to and from an Android application/device
  - Use Mobile Verification Toolkit (MVT) to investigate security incidents on Android devices
  - Perform log analysis on Android applications using the Logcat option and various available filters to determine the root cause and mitigate it efficiently
  - Use tools such as LogRabbit, Google Admin Toolbox Log Analyzer, and Logentries to analyze Android device logs

## 5.3 Stakeholders Involved

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Initiate evidence gathering and forensic analysis	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Analyze the scope of mobile-based security incident	CISO	Email, Phone, Text Message
	Information Security Manager	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message

## 5.4 Additional Information (if any)

**Note:** Refer to the following documents to fill the necessary details:

- l. Mobile-based Security Incidents Detection and Analysis Template.docx
- m. Checklist for Handling the Forensic Evidence Properly.docx
- n. Evidence Gathering and Forensic Analysis Form.docx

## 6. Eradication

### 6.1 Objectives

The main objective of this phase is to take appropriate measures to eradicate the incident and prevent recurrence in future.

### 6.2 Eradication Steps/Activities

*[Activities may differ based on organizational policies, but they are not limited to the following.]*

- Perform the following activities to eradicate the mobile security incident:
  - Perform repeated scans to completely remove the malicious application from the organizational network and devices
  - Use remote wiping techniques to delete organizational data from devices
  - Patch the identified vulnerabilities in devices to prevent similar incidents
  - Uninstall strange or suspicious applications installed on organizational mobile devices
  - Use tools such as Check Point's Harmony Mobile to prevent the download of malicious applications
  - Install mobile antivirus and security apps such as Norton Mobile Security, McAfee Mobile Security, and Kaspersky Antivirus & VPN
  - Enable built-in security features on Android devices
  - Uninstall APK files installed from third-party websites
  - Control or limit access to applications or services used by employees
  - Delete temporary files and applications and clear the recycle bin
  - Turn off the device and switch to the safe/emergency mode to eradicate the malware without triggering it
  - Reinstall the operating system or applications if the malware is persistent in nature
  - Update the operating system of devices
  - Change the device password and remove unnecessary permissions

- Logout from all applications before uninstalling them
- Remove unnecessary default add-ons and apps
- Clear the cache and downloaded files from devices
- Always restart the device in safe mode
- Activate Google Play Protect to detect and remove harmful apps
- Install antivirus tools such as AVG AntiVirus for Android to remove malware and other junk files
- Disable the auto Wi-Fi connection feature to prevent vulnerable network connections

### 6.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Develop an eradication plan ○ Perform technical and business analyses and create a prioritized eradication plan ○ Establish a communication strategy based on the eradication plan	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	Internal/External Communications Team	Email, Phone, Text Message
	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message
Eradication activities	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message

### 6.4 Additional Information (if any)

**Note:** Refer to the following documents to fill the necessary details:

- o. Eradication of Mobile-based Security Incidents Checklist.docx
- p. Incident Eradication Template.docx
- q. Incident Eradication Checklist.docx

## 7. Recovery

### 7.1 Objectives

The main objective of this phase is to recover the affected devices, network, and other resources from the incident impact and maintain business continuity.

### 7.2 Recovery Steps/Activities

*[Activities may differ based on organizational policies, but they are not limited to the following.]*

- Activities to recover from mobile-based security incident:
  - Ensure that all malware traces have been removed before restoration
  - Utilize data recovery tools such as Recoverit to recover lost data
  - Rebuild compromised devices using known good/trusted backups
  - Use data restore features such as recovery and Device Firmware Update (DFU) modes on devices
  - After removing the malware, update the applications and restore device functionalities
  - Enforce multifactor authentication mechanisms such as Google Authenticator and Authy instead of SMS authentication
  - Reconnect the rebuilt devices to the network and install the latest patches
  - Remove the affected and suspicious mobile applications
  - Restore mobile data from the cloud or local trusted backup
  - Check the functionality of all restored mobile devices
  - Continuously monitor mobile operations for abnormal behavior after restoring it to the normal condition
  - Strengthen perimeter security by changing access control rules after restoring the device
  - Change the Google account password previously associated with the infected device
  - Implement additional monitoring solutions to look for malicious activities originating from mobile devices

### 7.3 Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Recovery activities	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message

### 7.4 Additional Information (if any)

**Note:** Refer to the following documents to fill the necessary details:

- r. Recovery from Mobile-based Security Incidents Checklist.docx
- s. Incident Recovery Checklist.docx

## 8. Post-incident Activities

### 8.1 Objectives

The main objective of this phase is to create the necessary mobile-based security incident reports such as incident documentation, lessons learned, and incident impact assessment. Another objective of this phase is to close the investigation and disclose its details to respective stakeholders.

### 8.2 Activities Involved

- Perform mobile-based security incident post-mortem or incident review
- Create an after action report (AAR) that includes information such as what worked effectively, areas of improvement, and strategies for enhancing the response in case of similar mobile security incidents
- Conduct a lessons learned meeting to document all incident details; ensure that the following questions are answered in this meeting:
  - When and who detected the mobile-based security incident?
  - What happened exactly?
  - What caused the incident?
  - What challenges were encountered during the response process?
  - Which tools were effective during the response process?
  - To whom was the security incident reported?
  - Was the organization adequately prepared to handle the mobile incident?
  - How was the incident contained?
  - How were the impacted devices sanitized?

- What procedures were followed for recovery?
- Were the documented procedures followed by the response team?
- How well did the incident response team and management perform in resolving the mobile-based security incident?
- How should the incident response team and management respond to mitigate similar mobile security incidents in future?
- Were there any gaps in communicating the mobile security incident?
- Was the right amount of information shared with the right personnel?
- What are the tools and resources required to detect, analyze, and prevent similar mobile security incidents in future?
- Create concise and clear mobile security incident documentation in a standard format and get it reviewed by an editor
- Create an incident impact assessment report to determine all types of losses caused by the incident; this report must address the following, if required:
  - Financial losses incurred owing to the incident
  - Legal costs for investigating the case, lawyer's fees, etc.
  - Costs pertaining to the analysis of mobile security incident and recovery and installation of software or hardware
  - Implementation costs
  - Costs related to the damage of goodwill as well as loss of customer trust and reputation
- Officially close the mobile security incident investigation by informing the management and securely retain investigation reports considering the retention policy of the organization
- Disclose incident details to the respective stakeholders by consulting with the legal department of the organization
- If there were any lapses in the implemented IH&R plan, update the document according to the latest incident handling procedures
- Conduct technical and operational training on handling corporate data on mobile devices
- Review the entire network after recovery and document areas of improvements to be focused on by the administrators (regularly change passwords, update software, etc.)
- Validate the lesson learned documentation with the help of subject matter experts (SMEs)
- Incorporate some best practices against mobile security incidents

### 8.3 Stakeholders Involved/Communication Established

The stakeholders involved in the aforementioned activities and their communication modes are listed below:

Activities	Stakeholders Involved	Communication Mode/Channel
Conduct lessons learned meeting	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Create incident documentation	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Create an incident impact assessment report	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
Close the investigation officially	Information Security Manager	Email, Phone, Text Message
	IH&R Team	Email, Phone, Text Message
	Senior Management	Email, Phone, Text Message
Disclose incident details to the respective stakeholders	Information Security Manager	Email, Phone, Text Message
	Manager - Information Governance	Email, Phone, Text Message
	IT Manager/Director	Email, Phone, Text Message
	CISO	Email, Phone, Text Message
	Legal Team	Email, Phone, Text Message
	Human Resource	Email, Phone, Text Message
	Media	Email, Phone, Text Message
	Vendors	Email, Phone, Text Message
	Customers & General Public	Email, Phone, Text Message
	Business Partners	Email, Phone, Text Message
	Resilience Lead	Email, Phone, Text Message
	Business Continuity Lead	Email, Phone, Text Message
	Policy Area Lead	Email, Phone, Text Message



#### **8.4 Additional Information (if any)**

**Note:** Refer to the following documents to fill the necessary details:

- t. Incident Documentation Template.docx
- u. Incident Impact Assessment Report Template.docx
- v. Incident Closure Letter.docx
- w. Incident Disclosure Form.docx

#### **9. Appendix (if any)**