

Recovery from Mobile-based Security Incidents Checklist

Note: Prior to starting the recovery from mobile-based security incidents, Section 1 and Section 2 must be filled with required information.

Section 1: Details of the Organization

| | |
|--|--|
| Organization Name: | |
| Contact Number: | |
| Website: | |
| Address: | |
| <i>Additional Contact Information:</i> | |
| | |

Section 2: Details of the Incident Responder

| | | | |
|---|--|-------------------------------|--|
| Date Report Received: | | Date Report Processing Began: | |
| Name: | | Report Number: | |
| Title: | | Department: | |
| Email Address: | | | |
| Phone Number and, If Applicable, Extension: | | | |

| Section 3: Checklist for Recovering from Mobile-based Security Incidents | |
|--|--------------------------|
| Actions | Completed |
| Whether the compromised systems and devices are rebuilt using a known good or trusted backup | <input type="checkbox"/> |
| Whether a data recovery tool such as RecoverIt is utilized to recover any lost data | <input type="checkbox"/> |
| Whether all traces of the malware have been removed before the restoration of affected devices | <input type="checkbox"/> |
| Whether data from other external storage components such as SIM cards, SD cards, etc., are collected for further investigation | <input type="checkbox"/> |
| Whether the data restore features such as recovery mode and Device Firmware Update (DFU) mode are used on devices | <input type="checkbox"/> |
| Whether the OS and anti-virus software are updated with the latest patches | <input type="checkbox"/> |
| Whether advanced mobile threat prevention tool such as Harmony Mobile is installed on the devices | <input type="checkbox"/> |
| Whether multi-factor authentication mechanisms such as Google Authenticator or Authy are enforced, instead of SMS authentication | <input type="checkbox"/> |
| Whether the IH&R teams continuously monitored the affected mobile device for some time after restoring it | <input type="checkbox"/> |
| Whether the devices are rebuilt and reconnected to the network after applying the latest patches | <input type="checkbox"/> |
| Whether suspicious mobile applications are removed before restoring the device | <input type="checkbox"/> |
| Whether the passwords of all affected accounts are changed | <input type="checkbox"/> |
| Whether the mobile data is safely restored from the cloud or local trusted backup | <input type="checkbox"/> |
| Whether the functionality of all restored mobile devices is verified | <input type="checkbox"/> |
| Whether additional monitoring solutions are deployed to look for suspicious activities of mobile devices | <input type="checkbox"/> |