

Incident Response Checklist



This checklist walks you through the steps to take and the order to take them if a breach should occur.

Phase One Discovery and Initial Organization

- Alert appropriate leaders** in the company of the incident. Record date, time and method of the alert.
- Notify your organization's internal Incident Response Team (IRT).**
Members often include:
 - Information Technology/Information Security
 - Legal/Compliance
 - Human Resources
 - Public Relations
 - Customer Service
 - Executive
- Identify an incident lead** who will serve as your project manager.
- Convene an IRT conference call** for initial triage.
- Contact external privacy counsel** to make them aware of the incident.
- Collaborate with counsel** on proper role and implementation of the attorney-client privilege in the context of a cybersecurity investigation.
- Consider hiring external computer forensic** investigators, depending on internal resource availability and complexity of incident.
- Consider notifying law enforcement** per your incident response plan.

Phase Two Initial Investigation

- Identify, document, and limit scope** of security compromise to the extent possible within 24-48 hours.
- Ensure your actions won't trigger more issues**, as some actions may alert criminals that you have discovered them and cause them to speed up their actions.
- Preserve any evidence** related to the ongoing security incident.

Phase Three Incident Containment

- Confirm the full scope** of the security compromise.
- Contain the security breach** to stop any possible flow, access, or disclosure of data to unauthorized recipients.
- Document containment effort and results** for post-mortem evaluation and future planning.

Phase Four In-Depth Investigation

- Perform root cause analysis** to learn how to mitigate against future issues.
- Classify the incident** according to its type (e.g. email, theft, etc.).
- Identify the data compromised**, if any, which might include:
 - Regulated Personal Information
 - Social Security Numbers
 - Biometric Data

- Payment Card Information
- Financial Account Data
- Medical Information
- Usernames & Passwords
- Contact Information (Name, Address, Email Address, Phone)
- Driver's License Numbers
- Other Sensitive Information
- Preferences, Purchase History
- Other Information linked to a person
- Identify impacted individuals**, and where they reside.
- Identify the nature of any unauthorized recipients or access**, which might be:
 - Employee Acting In Good Faith
 - Suspected Business Partner Acting In Bad Faith
 - Suspected Business Partner Acting In Good Faith
 - Trustworthy Recipient who normally receives information of this nature
 - Unknown Individuals, but definite disclosure
 - Lost Information that may not have been disclosed
 - Known Bad Faith Actor
 - Departing/Former Employee
- Assess known or potential use** of compromised information.
- Make security updates** before notification if necessary.

Phase Five Notification

Before notification

- Consult your crisis communication plan** for potential media inquiries and make any necessary adjustments.
- Consider an internal notification plan** for effective communication to company leadership, board of directors, or others who should be notified before the public.
- Prepare for inquiries** from impacted individuals and assess the need for a call center.
- If it has not already been done in Phase 1, notify any necessary law enforcement**, such as local, FBI, Secret Service, or other authority.
- Notify impacted individuals** if required by law or otherwise recommended by privacy counsel. Make sure notification includes:
 - Any information required by law.
 - Government agency harm prevention resource information.
- Consider whether to include an offer** of identity theft prevention or credit monitoring services for impacted individuals.
- Notify state attorneys general and government agencies** as required by law.
- Notify other parties as required** by information at issue, such as pursuant to contractual obligation.

- Evaluate feedback** from notifications and determine if additional steps or notifications may be required.

Phase Six Post-notification

- Draft disclosures** to investors, shareholders, SEC, etc.
- Analyze potential cost recovery** from any third-parties responsible for the security breach.
- Work with your Resilience claims team** to finalize your insurance claim recovery.
- Consider upgrades and other measures** that could improve future cyber resilience.
- Analyze incident response plans and make improvements** in light of experience and lessons learned.
- Prepare final reports**, including:
 - Executive summary of what happened and how the IRT responded. Details should include notification measures and steps taken to prevent future events.
 - Detailed technical report with background of the event; evidentiary backup for analysis, decisions, and conclusions; and evidence of all preventive measures.