KAMMCO

# INFORMATION SECURITY INCIDENT RESPONSE CHECKLIST

This checklist highlights key steps in responding to a potential compromise of sensitive information in all forms, whether electronic, paper, verbal, etc. As every security incident is different, not all components of this checklist may be applicable to each type of security incident. This document does not provide legal advice, and it is recommended that legal counsel be consulted given the potential legal implications of a privacy or data security incident.

## TABLE OF CONTENTS



Reviewed 2020

## DETECTING AND REPORTING INCIDENTS

- ☐ **Do not panic!** **Do not** turn off or reboot any affected systems.
- ☐ Take notes (e.g. date, time, systems/data affected, who discovered).
- ☐ Report the incident to a member of the Incident Response Team (IRT).
- ☐ Secure the scene to preserve evidence.
- ☐ Restrict actions taken on affected systems to forensic experts.

## THE FIRST 24 HOURS: ENGAGING THE IRT & CONDUCTING INITIAL ANALYSIS

- ☐ Engage the Incident Response Team (IRT) Leader and appropriate team members.
- ☐ Review Incident Response Plan.
- ☐ Document known facts in the Information Security Incident Report Form including:
  - ☐ Date and time of incident detection and reporting
  - ☐ Incident detector's contact information
  - ☐ Location of the incident
  - ☐ Systems, applications, and/or data possibly at risk
  - ☐ Type of incident detected
  - ☐ General description of incident
  - ☐ Names and contact information of others involved
  - ☐ Any actions taken since incident detection
  - ☐ Whether the incident is contained (and, if so, when/how)
  - ☐ Any additional relevant information known at the time
- ☐ Promptly investigate and conduct initial analysis.
- ☐ Confirm the incident.
  - ☐ Incident real v. perceived
  - ☐ Incident ongoing v. contained
- ☐ Assign Threat Level and prioritize incident based on potential impact:
  - ☐ **Level 1** – Neither mission critical systems/resources nor Confidential Information (CI) or Personal Information (PI) were impacted.
  - ☐ **Level 2** – Critical systems/resources and/or CI/PI may be at risk.
  - ☐ **Level 3** – Mission critical systems/resources and/or CI/PI have been impacted.
- ☐ Report to senior management (as appropriate).
- ☐ Consult with legal counsel.
- ☐ Restrict Communications.
  - ☐ Restrict knowledge of event to IRT team and on a "need to know basis."
  - ☐ Instruct team not refer to incident as a "breach."
  - ☐ Communicate verbally and use email only when necessary.
  - ☐ When using email, encrypt messages and copy counsel.
  - ☐ Mark written communications as follows: "Privileged and Confidential: Attorney-Client Privileged Communication. This document was prepared at the direction of counsel for the purpose of obtaining legal advice."

- ☐ Notify insurance carrier(s) (if appropriate).
  - ☐ Review insurance policies.
  - ☐ Notify insurance broker(s).
  - ☐ Notify insurance carrier(s).
  - ☐ Identify resources available under policies (e.g. forensics, legal, vendors).
- ☐ Determine whether to engage external experts and/or vendors such as:
  - ☐ Legal counsel with experience handling data breaches
  - ☐ Forensics investigators (retain under guidance of counsel)
  - ☐ Crisis communications / PR firm
  - ☐ Response vendors (e.g. notification, call center, identity protection)
  - ☐ Law enforcement (based on advice of counsel) and, if so, identify the appropriate agency (e.g. Secret Service, FBI, local police)
- ☐ Review contracts with vendors (if any).

## PRESERVING EVIDENCE

- ☐ Do not turn off or reboot any potentially affected systems.
- ☐ Secure the scene and prevent access to affected systems to maintain the integrity of the evidence. Restrict action taken on affected systems to forensic experts, (e.g. disconnecting affected systems from the Internet).
- ☐ Preserve all evidence including logs and surveillance tapes.
- ☐ Send preservation letters to third parties (e.g. service and cloud providers).
- ☐ Track the chain of custody (e.g. list everyone who had access to the systems, in order, as well as, actions taken) for all physical and digital data.
- ☐ Identify the systems, applications, and data (type and classification) compromised and back up affected systems to allow further analysis of the system, including any forensic analysis (if needed).

## INVESTIGATING AND DOCUMENTING STEPS TAKEN

- ☐ Investigate to determine nature, scope, and impact of incident.
- ☐ Document findings and steps taken in the Incident Security Incident Report Form including:
  - ☐ Systems & applications (type and classification) or processes and procedures impacted
  - ☐ Whether CI/PI was compromised
  - ☐ Data elements potentially compromised:
    - ☐ Name
    - ☐ Address
    - ☐ Telephone
    - ☐ Email
    - ☐ Social Security number
    - ☐ Drivers' License number
    - ☐ Other government issued ID number
    - ☐ Date of birth
    - ☐ Financial account number
    - ☐ Credit card number

- ☐ Debit card number (with/without PIN)
- ☐ Medical information
- ☐ User name and password
- ☐ Criminal background records
- ☐ Other: _____

☐ Whether data was encrypted and, if so, if encryption key was compromised

☐ Potential scope of incident

- ☐ Number of persons affected: _____
- ☐ Number of records affected: _____

☐ Persons affected

- ☐ Employees, customers, patients, students, vendors
- ☐ Past, present, or future

☐ Critical dates:

- ☐ Date/time when incident occurred (if known)
- ☐ Date/time the incident was discovered
- ☐ Date/time the incident was reported

☐ Names and contact information for person(s) who:

- ☐ Discovered the incident
- ☐ Reported the incident
- ☐ Others with knowledge of the incident

☐ Physical location and/or network of affected systems

☐ Type of incident

- ☐ Malicious code (e.g. worm, virus, Trojan)
- ☐ Unauthorized computer or network access
- ☐ Network attack (e.g. denial of service)
- ☐ Violation of privacy or data security policies or procedures
- ☐ Social engineering (e.g. phishing)
- ☐ Inadvertent disclosure of personal information (e.g. posting on a website or public forum, email sent to wrong person or without encryption)
- ☐ Abuse or misuse of corporate assets
- ☐ Compromised system or user credentials
- ☐ E-mail abuse
- ☐ Internet abuse
- ☐ Media leak damage
- ☐ Lost or theft of a PC, laptop, cell phone or other electronic storage device
- ☐ Lost, stolen, or missing hard-copy documents or media
- ☐ Other: _____

☐ Source of incident (e.g. type of threat actor)

☐ Description of how incident happened

☐ Whether the incident has been contained and, if so, when/how

## RESPONDING TO THE INCIDENT

- ☐ Identity response objectives (e.g. controlling costs, minimizing reputational harm, protecting affected customers).
- ☐ Formulate response strategy based upon scope and potential impact.
- ☐ Identify and prioritize response tasks.
- ☐ Determine response budget and allocate resources.
- ☐ Continue documenting steps.
- ☐ Keep senior management updated on response and potential impact.

### Containing, Eradicating, and Recovering from the Incident

- ☐ Evaluate appropriate containment and mitigation strategies based on:
  - ☐ Potential damage to resources
  - ☐ Need for preservation of evidence
  - ☐ Service availability
  - ☐ Time and resources needed to implement the strategy
  - ☐ Effectiveness of the strategy
  - ☐ Duration of the solution
- ☐ Take steps necessary to contain the incident and limit further data loss (if possible).
- ☐ Secure any affected IT/IS systems or information.
- ☐ Eradicate components of the incident or malware (if necessary).
- ☐ Restore any loss of information.

### Return to Normal & Secure Functioning IT/IS Systems & Business Operations

- ☐ If data was corrupted or destroyed, perform a reliable recovery.
- ☐ Take steps to eliminate the vulnerability and mitigate future security incidents (e.g. patch systems, change passwords, update anti-virus).
- ☐ Preserve evidence and document actions taken to contain, eradicate and recover impacted systems/data and prevent further harm or occurrences.

### Determining Legal Obligations

- ☐ Consult legal counsel experienced in privacy and data breach laws.
- ☐ Assess duty to notify affected persons/third parties under federal/state laws.
- ☐ Determine whether there is a legal duty or contractual obligation to notify:
  - ☐ Affected persons
  - ☐ Media
  - ☐ Regulators
  - ☐ Law enforcement
  - ☐ Other third parties (e.g. vendors, business partners, licensing agencies, data owners, payment card merchant banks/brands)

- ☐ Credit Reporting Agencies
- ☐ Other

☐ Determine regulatory deadline for notifications.

☐ Prepare notification timeline and assign tasks.

☐ Evaluate whether to notify regulators even if not required (based upon advice of counsel).

☐ Determine legal obligations to provide identity theft mitigation services.

☐ Identify other legal obligations (e.g. conduct an incident risk assessment).

## Determining Remediation Strategies for Affected Persons

☐ Identify harm posed to affected persons based on data elements compromised (e.g. name, Social Security number, medical information, payment card).

☐ Evaluate whether to offer identity theft mitigation services to affected persons.

☐ Identify identity theft protection vendor or review vendor contracts (if any).

☐ Identify appropriate identity theft protection services to offer (if any).

☐ Determine duration for coverage period (e.g. 1 year, 2 years).

## Developing Communication Plans

☐ Determine whether to engage crisis communications / PR firm.

☐ Formulate internal and external communication plans (who, what, how, when):

- ☐ Identify who needs to be notified (consider all external and internal audiences).
- ☐ Determine what needs to be shared about the incident.
- ☐ Determine how/when to notify employees/internal resources.
- ☐ Instruct employees and internal resources on communications protocols.
- ☐ Determine how to communicate external message (e.g. press release, website).
- ☐ Prepare communication timeline.

☐ Prepare communications.

- ☐ Prepare holding statement (if any).
- ☐ Prepare press release (if any).
- ☐ Prepare website release (if any).
- ☐ Prepare notification letters (if any).

☐ Prepare media communication strategy.

- ☐ Identify contact to address media and other inquiries about the incident.
- ☐ Train media contact/spokesperson.
- ☐ Prepare media contact for responses to common questions:
  - ☐ What happened?
  - ☐ Who attacked you and why?
  - ☐ How did the attack occur and why was it successful?
  - ☐ How widespread is the incident?
  - ☐ What measures are you taking to determine what happened and prevent against future occurrences?

- ☐ What is the impact of this incident?
- ☐ Was any personally identifiable information compromised?
- ☐ What steps are you taking to contain the harm and protect those affected?
- ☐ What is the estimated cost of this incident?

☐ Prepare social media communication plan.

- ☐ Identify and prepare contact who will respond to social media inquiries (e.g. the organization's website, Facebook, Twitter, Blogs) and emails.
- ☐ Designate team member to monitor social media and press.
- ☐ Prepare social media messages.

## Preparing Call Center/Customer Support

☐ Anticipate volume of calls based on scope/size of event.

- ☐ Anticipate types of questions from persons affected by incident.
- ☐ Prepare to respond to others who hear about incident.
- ☐ Consider facts that may increase calls (e.g. employee breach, concentrated population, publicity).

☐ Determine whether calls will be handled in-house or by external call center.

☐ Identify call center vendor (if needed) or review vendor contract (if any).

☐ Prepare scripts for call center agents.

☐ Prepare FAQs for call center agents.

☐ Develop escalation process (e.g. callers demanding to speak to a representative of your organization or threatening legal action).

☐ Determine whether agents must answer calls in multiple languages.

☐ Determine required dates/times of availability for call center staff.

☐ Ensure call center "go live" coincides with press release and/or notifications.

☐ Train call center agents.

☐ Test/QA the agents and train/modify scripts as necessary.

## Notifying Affected Persons and Third Parties

☐ Determine how the notification process will be handled:

- ☐ Via mail
- ☐ Via email
- ☐ Via substitute notice (e.g. press release, website or publication)

☐ For mail or email notifications:

- ☐ Prepare timeline (e.g. notifications for large events may be staggered).
- ☐ Determine whether to mail notifications internally or engage a vendor.
- ☐ Identify external notification vendor if needed, and review contract.
- ☐ Determine number of letter versions based on variations in state laws.
- ☐ Prepare notification letter templates (with advice of legal counsel).
- ☐ Prepare address file.

- ☐ Determine whether addresses are current or will need verification.
- ☐ Determine whether letters will need to be translated into multiple languages.
- ☐ Determine how to handle returned mail (for mailed notifications).
- ☐ Prepare additional notification materials (e.g. logo, signature graphic).
- ☐ Determine whose signature will be provided in the letters.
- ☐ Obtain approval of notification letters by senior management/signatory.

☐ For substitute notice:

- ☐ Prepare language for notice (with advice of counsel).
- ☐ Determine timing of notice.
- ☐ Obtain approval of notification letters by senior management/signatory.

## CONDUCTING POST-INCIDENT REVIEW & IMPROVING INCIDENT RESPONSE PLAN

- ☐ Review incident response to understand cause and areas for improvement.
- ☐ Evaluate administrative, technical and physical safeguards and strengthen as needed.
- ☐ Review information security systems, policies and procedures, and workflows and improve as needed.
- ☐ Update training programs to reflect changes and improvements.
- ☐ Summarize and document all “lessons learned.”
- ☐ Evaluate response and identify areas for improvement.
- ☐ Evaluate the IRT communication plan, assess how well it worked and identify areas of improvement.
- ☐ Update the IRP based upon findings.
- ☐ Review and update the risk assessment to reflect the new information.
- ☐ Conduct regular updates and training to reduce risks and ensure organization is prepared to effectively respond to future events.