DATA INCIDENT
Initial Response Reference Guide

✓ Identify + Verify Incident

Identify affected systems.

Determine nature of the data maintained in those systems.

Determine type of incident:

- Internal or external disclosure
- Inside or outside actor
- Malicious attack or accident

Perform Risk Assessment (likelihood of harm to individuals, number of individuals affected).

Determine whether personally identifiable information ("PII") was affected and the data elements possibly at risk (name, date of birth, Social Security number, or credit card number).

✓ Contain + Mitigate Incident

Limit further data loss or intrusion by:

- Segregating affected systems
- Deleting hacker tools
- Taking affected hardware offline
- Changing passwords, administrative rights, access codes, or physical locks

Determine vulnerabilities of other systems.

✓ Execute Incident Response Plan (IRP). If no IRP, Assemble Incident Response Team.

Internal: Identify incident lead and include a representative(s) from different areas of the organization (executive, public relations, marketing, operations, information technology and human resources). Appoint someone responsible for keeping a response log of the actions taken during the internal investigation.

External: Outside legal counsel and service providers (forensic, public relations, identity theft).

✓ Investigate + Analyze Incident

Conduct the incident investigation under attorney-client privilege.

Institute protocols for communications (internal, external, with law enforcement) to prevent information leaks.

Preserve all data and evidence, including forensic evidence, for later examination or if needed in the event of any later legal or regulatory action.

✓ Consider Whether + When to Notify Law Enforcement or Regulatory Authorities

Learn More ▶ keglerbrown.com/datasecurity

KEGLER
BROWN
HILL+
RITTER

DATA INCIDENT
Initial Response Reference Guide

✓ Collect Data + Document Incident

Collect information about the incident itself, including:

- How the incident was discovered
- Nature of the incident
- Date and time of the incident
- Duration and location of the incident
- Method of intrusion
- Compromised systems or files

Collect details about the compromised data, including:

- List of affected individuals
- Affected data elements
- Number of records affected
- Whether PII was actually accessed
- Whether any of the data was encrypted

✓ Analyze Legal Implications

Review legal requirements (HIPAA, GDPR, State law).

Identify the jurisdictions where any affected persons may reside to assess which breach notification laws may be triggered.

Identify whether the type of data compromised triggers additional statutory or sector-specific notification obligations.

Review relevant contracts and policies.

Based on the analysis of these factors, determine whether the incident triggers any notification obligations as to:

- Affected individuals
- Third-party business partners or vendors
- State attorneys general or other regulatory agencies, such as the Office of Civil Rights in the event of a HIPAA-covered incident
- Law enforcement
- Consumer reporting agencies
- Media outlets

Review the organization's insurance coverage to determine any relevant coverage and notify carriers.

Determine the organization's indemnification obligations or rights.

Assess the risk of litigation or regulatory action against the organization.

✓ Develop Internal + External Inquiry Response Plan

✓ Prepare + Execute Notification Plan

✓ Post-Notification + Response Review

Learn More ▶ keglerbrown.com/datasecurity

KEGLER
BROWN
HILL+
RITTER