Data Breach Response Checklist

PRACTICAL LAW INTELLECTUAL PROPERTY & TECHNOLOGY

A Checklist outlining the steps for an organization to follow in responding to a breach of personally identifiable information (PII). It addresses key steps to take concerning verification, containment, investigation and analysis, notification and post-notification review.

PRELIMINARY CONSIDERATIONS

- Responding to a data breach that exposes individuals' personally identifiable information (PII) typically involves the following stages:
  - verification;
  - containment and mitigation;
  - investigation and analysis;
  - notification; and
  - post-notification, including a review of the breach to improve processes.
- Data breach response is typically not purely linear, as these stages and the activities associated with these stages frequently overlap.
- Keep a record of any actions the organization takes in responding to the incident. Some laws, including the Health Insurance Portability and Accountability Act (HIPAA), may require keeping an incident log.
- Preserve any evidence that may be relevant to any potential regulatory investigation or litigation.

For detailed guidance on responding to a data breach, see *Practice Note, Breach Notification (http://us.practicallaw.com/3-501-1474)*. For state-specific breach notification requirements, see *Data Breach Notification Laws: State Q&A Tool (http://us.practicallaw.com/3-578-0925)*.

VERIFY THE DATA BREACH

- Identify the affected systems or hardware (such as a lost laptop or USB drive).
- Determine the nature of the data maintained in those systems or on the hardware.
- Determine the type of incident, such as whether the disclosure was:
  - internal or external;
  - caused by a company insider or outside actor; and
  - the result of a malicious attack or an accident.
- Determine whether the incident exposed or is reasonably likely to have exposed data.
- Determine whether PII was affected and the data elements possibly at risk, such as name, date of birth or Social Security number.

CONTAIN AND MITIGATE THE DATA BREACH

As soon as an organization verifies a breach has occurred, it should take all necessary steps to contain the incident and limit further data loss or intrusion, such as:

- Identify the system, application and information compromised.
- Identify and take immediate action to stop the source or entity responsible, for example by:
  - taking affected machines offline;
  - segregating affected systems;
  - deleting hacker tools; and
  - immediately securing the area if the breach involves a physical security breach.
- Determine whether other systems are under threat of immediate or future danger.

Determine whether to implement additional technical measures to contain the data breach, such as changing locks, passwords, administrative rights, access codes or passwords.

© 2015 Thomson Reuters. All rights reserved.

CONVENE THE DATA BREACH RESPONSE TEAM

- Convene the data breach response team (see *Practice Note, Breach Notification: Preparing for and Responding to a Data Security Breach (http://us.practicallaw.com/3-501-1474)*) when there is a reasonable belief that a breach may have occurred. The response team is responsible for:
  - managing and coordinating the organization's overall response efforts; and
  - investigating and responding to the data breach in accordance with the organization's incident response plan.
- The data breach response team generally should:
  - determine the scope of an internal investigation (see *Investigate and Analyze the Data Breach*);
  - collect data related to the breach (see *Collect Data*);
  - consider immediate notification of outside counsel, especially if the organization does not have in-house counsel;
  - consider whether and when to notify law enforcement or regulatory authorities (see *Consider Communications with Regulators and Law Enforcement*);
  - consider whether it should engage specialized third-party consultants to assist in capturing relevant information and performing a forensic analysis;
  - appoint someone responsible for keeping a response log that records the actions taken during the investigation;
  - institute and manage internal and external communications protocols (see *Develop a Communications Plan*); and
  - conduct follow up reviews on the effectiveness of the company's response to an actual attack (see *Post-Notification and Breach Response Review*).

INVESTIGATE AND ANALYZE THE DATA BREACH

When investigating a data breach, the response team should:

- Institute communications protocols, such as communicating by telephone where possible, to prevent information leaks.
- Take steps to conduct the incident investigation under attorney-client privilege.
- Preserve all data and evidence, including forensic evidence, for later examination or if needed in the event of any later legal or regulatory action.

COLLECT DATA

- Keep in mind that collecting data is a continuous process.
- To effectively collect relevant data, the organization will likely have work with its IT department or engage a forensics vendor.
- Collect information about the breach itself, including:
  - how the breach was discovered;
  - the nature of the breach (for example, whether systems were compromised or hardware lost);
  - the date and time of the breach;
  - the duration and location of the breach;
  - the method of system intrusion;
  - the compromised systems or files; and
  - whether PII was actually accessed.
- Collect details about the compromised data, including:
  - a list of affected individuals;
  - the affected data elements;
  - the number of records affected; and
  - whether any of the data was encrypted.

ANALYZE THE LEGAL IMPLICATIONS

- Once the basic facts are known, analyze the legal issues stemming from the breach. The legal analysis should be conducted at the direction of internal or external counsel.
- To assess whether the breach may trigger individual and regulatory notification obligations, in addition to the data elements affected, determine:
  - the likely use of or access to the compromised data;
  - for purposes of some laws, the likelihood of harm to individuals; and
  - the number of persons likely affected.
- Identify the jurisdictions where any affected persons may reside to assess which state (or foreign) breach notification laws may be triggered.
- Identify whether the type of data compromised, for instance medical information, triggers additional statutory obligations under state law.
- Identify whether the organization is subject to sector-specific federal notification obligations, for instance if it is a financial institution covered by the banking regulators' interagency guidance or is a HIPAA-covered entity.
- Review relevant contracts and policies.
- Based on the analysis of these factors, determine whether the breach triggers any notification obligations (see *Notification*) as to:
  - affected individuals;
  - third-party business partners or vendors;
  - state attorney generals or other regulatory agencies, such as the Office of Civil Rights in the event of a HIPAA-covered breach (see *State Agency Notice Requirements for Data Breaches Chart (http://us.practicallaw.com/5-501-9110)*);
  - law enforcement (see *Practice Note, Breach Notification: Contacting Law Enforcement (http://us.practicallaw.com/3-501-1474)*); or
  - consumer reporting agencies.
- Review the organization's insurance coverage to determine any relevant coverage and notify carriers.
- Determine the organization's indemnification obligations or rights, including whether:
  - any third parties have any obligations to the organization; and
  - the organization has any indemnification obligations to third parties.
- Assess the risk of litigation or regulatory action against the organization.
- Determine whether the organization should take any employment action against any responsible employees as a result of the breach.

© 2015 Thomson Reuters. All rights reserved.

DEVELOP A COMMUNICATIONS PLAN

Before any communications, develop a communications plan approved by the organization's media relations professionals, executives and counsel that:

- Ensures timely and coordinated execution of external communications and notifications.
- Avoids disseminating incomplete information or information that has not been thoroughly vetted.
- Addresses how the organization responds to inquiries about the breach (see *Prepare an Inquiry Response Plan*).
- Tailors communications to each of the key audiences, including:
  - the organization's employees (see *Consider Internal Communications*);
  - affected individuals (see *Plan for Communications with Affected Individuals and Notification*);
  - the media (see *Plan for Media Communications*);
  - vendors or other third parties (see *Address Communications with Third Parties*); and
  - law enforcement and regulators (see *Consider Communications with Regulators and Law Enforcement*).

PREPARE AN INQUIRY RESPONSE PLAN

- Develop an inquiry response plan that takes into account the size of the breach and the number of individuals affected.
- Ensure that the plan addresses:
  - whether to handle inquiries internally or by engaging a call center vendor;
  - whether to post a statement on the organization's website, which in some cases may be required by law; and
  - the methods of communication with each of the key audience groups.

CONSIDER INTERNAL COMMUNICATIONS

In communicating with employees and other internal stakeholders:

- Limit communications regarding the details of the incident on a need-to-know basis.
- Notify employees and other internal stakeholders as soon as the data breach is contained and basic facts are known.
- Consider whether employees are also affected persons that must receive individual notification.
- Issue a policy statement to employees regarding external communication with media or third parties.

PLAN FOR MEDIA COMMUNICATIONS

- Attempt to avoid news of the data breach reaching the media before notifying affected individuals (see *Notification*).
- Prepare a media holding statement to ensure that the organization is prepared to make an announcement quickly if required.
- Draft a media and web statement or press release based on incident-specific facts.
- Designate a contact person on the data breach response team to handle media and law enforcement inquiries.

CONSIDER COMMUNICATIONS WITH REGULATORS AND LAW ENFORCEMENT

- Consider whether and when to contact law enforcement (see *Practice Note, Breach Notification: Contacting Law Enforcement*).
- Keep in mind that law enforcement authorities may require a delay in the notification to affected persons or a release of public information if those activities may hamper law enforcement investigations.
- Consider whether the organization must, or if it is otherwise advisable to, communicate with any regulatory authority regarding the incident.
- Both counsel and executives should be included in developing communications with regulators.

ADDRESS COMMUNICATIONS WITH THIRD PARTIES

If the data breach affected PII the organization maintains for third-parties:

- Involve executives and counsel in developing the approach to communications.
- Reach out to data owners as soon as possible.
- Pre-determine whether:
  - individual notification may be necessary; and
  - the organization must by contract or is otherwise willing to notify on the data owner's behalf.
- Foster a cooperative relationship with the data owners to secure sensitive data and mitigate the damage that may arise from the data breach.
- Designate an individual on the data breach response team to handle communications with data owners and other affected third parties.

PLAN FOR COMMUNICATIONS WITH AFFECTED PERSONS

- Prepare for inquiries from affected individuals after the breach becomes public, usually at the time that notification is sent (see *Prepare an Inquiry Response Plan*).
- An effective communications plan should include, as appropriate based on the scope of the breach:
  - setting up a dedicated toll-free phone number to field calls and questions from affected individuals;
  - preparing a call center script, training call center representatives and establishing an escalation process for inquiries that the front-line call center cannot handle ;
  - preparing frequently asked questions (FAQs) for responding to affected individuals' inquiries;
  - posting information on the organization's website; and
  - designating an individual from the data breach response team to field inquiries that do not come through the toll-free number.

NOTIFICATION

If notification is necessary:

- Develop a notification plan (see *Prepare a Notification Plan*).
- Ensure that notification is executed in a timely and legally sufficient manner (see *Execute the Notification Plan*).

© 2015 Thomson Reuters. All rights reserved.

PREPARE A NOTIFICATION PLAN

- Identify notification obligations based on analysis of legal requirements (see *Analyze the Legal Implications*).
- Determine the parties or entities that should be notified before notification to affected individuals, such as:
  - law enforcement;
  - regulatory agencies (see *State Agency Notice Requirements for Data Breaches Chart (http://us.practicallaw.com/5-501-9110)*); or
  - credit reporting agencies (see *Practice Note, Data Breach Notification: Notice to Government Entities and Credit Reporting Agencies (http://us.practicallaw.com/3-501-1474)*).
- Consider whether the organization can handle notification logistics internally or whether it must engage third-party notification vendors for:
  - printing and mailing letters; or
  - operating a call center to respond to inquiries (see *Prepare an Inquiry Response Plan*).
- Determine whether to offer remediation services to affected individuals, such as:
  - credit monitoring services; or
  - identity theft insurance.
- (See *Practice Note, Data Breach Notification: Determining Whether to Offer Remediation Services (http://us.practicallaw.com/3-501-1474)*.)
- Prepare a notification timeline or schedule.

EXECUTE THE NOTIFICATION PLAN

While specific legal requirements may depend on the facts of the breach, typically, when notifying individuals, an organization should:

- Prepare and maintain a list or database of persons to be notified that includes:
  - the person's name and address;
  - other contact and identifying information for the person;
  - the affected data elements; and
  - the notification status.
- Determine the method of notification, considering that applicable law or contracts may require certain modes of communication.
- Draft template notification letters to affected persons that take into account:
  - the specific content requirements for the notifications, which are typically dictated by statute; and
  - whether the affected person is a minor or is deceased, in which case the letters should be directed to personal representatives or guardians and may differ as to whether and what mitigation products are offered.
- Draft notification letters, if they are required, to:
  - credit reporting agencies; and
  - regulatory or law enforcement agencies.
- Draft substitute notice if permitted or required by law.

For more information on drafting data breach notification letters, see *Standard Document, Data Security Breach Notice Letter (http://us.practicallaw.com/3-501-7348)*.

POST-NOTIFICATION AND BREACH RESPONSE REVIEW

- Consider whether a Securities and Exchange Commission (SEC) disclosure is required (see *Article, Board Oversight of Cybersecurity Risks: Disclosing Cybersecurity Risks: SEC Guidance (http://us.practicallaw.com/5-558-2825)* and *Standard Clause, Sample Risk Factor: Cyber Security (http://us.practicallaw.com/9-506-9947)*).
- Review applicable access controls, policies and procedures and determine whether to take any actions to strengthen the organization's security program (for more information on assessing security programs, see *Practice Note, The NIST Cybersecurity Framework (http://us.practicallaw.com/5-599-6825)* and *Common Gaps in Information Security Checklist (http://us.practicallaw.com/3-501-5491)*).
- Review the response to determine whether any changes should be made to the organization's incident response policy or procedures.

ABOUT PRACTICAL LAW

Practical Law provides legal know-how that gives lawyers a better starting point. Our expert team of attorney editors creates and maintains thousands of up-to-date, practical resources across all major practice areas. We go beyond primary law and traditional legal research to give you the resources needed to practice more efficiently, improve client service and add more value.

If you are not currently a subscriber, we invite you to take a trial of our online services at **practicallaw.com**. For more information or to schedule training, call **646.562.3405** or e-mail **ustraining@practicallaw.com**.

11-13

© 2015 Thomson Reuters. All rights reserved. Use of Practical Law websites and services is subject to the Terms of Use (http://us.practicallaw.com/2-383-6690) and Privacy Policy (http://us.practicallaw.com/8-383-6692).