BCLP. Client Intelligent

**Insights**

# WHAT SHOULD BE INCLUDED IN A DATA BREACH INCIDENT RESPONSE PLAN?

Jan 09, 2020

As of January 1, 2020, California became the first state to permit residents whose personal information is exposed in a data breach to seek statutory damages between $100-$750 per incident, even in the absence of any actual harm, with the passage of the California Consumer Privacy Act ("CCPA"). The class actions that follow are not likely to be limited to California residents, but will also include non-California residents pursuing claims under common law theories. A successful defense will depend on the ability of the breached business to establish that it implemented and maintained reasonable security procedures and practices appropriate to the nature of the personal information held. The more prepared a business is to respond to a breach, the better prepared it will be to defend a breach lawsuit. To help our clients prepare for the CCPA, Bryan Cave Leighton Paisner is issuing a series of data security articles to empower organizations to focus on breach readiness.

## What Should be Included in a Data Breach Incident Response Plan?

An incident response plan explains how an organization handles security events, security incidents, and security breaches. Among other things, the plan helps employees from different departments understand the role that they are expected to play when investigating a security incident and identifies other people within the organization with whom they should be coordinating. The plan also can help educate employees concerning what they should and should not do when faced with a security incident and can provide them with a reference guide for resources that may help them effectively respond to an incident or breach.

Incident response plans take a variety of forms, and there is no mandated structure. The following topical recommendations, however, may help you draft an incident response plan or evaluate the thoroughness of one that already exists:

- **Definition of Security Event, Incident, and Breach**. Consider explaining the difference between an event, incident, and breach so those in the organization involved with incident response understand the distinction.

- **Security Event Escalation**. By their very nature, security events are relatively common occurrences. Only a small percentage of events will become incidents, and an even smaller percentage of events will ultimately become breaches. Nonetheless, it is important to explain the process under which an event should be escalated to an incident, or a breach, and the impact that such an escalation has on who within the organization needs to become involved in an investigation and how the investigation should be handled.

- **Responsibilities For Conducting an Incident Investigation**. The plan should explain who within the organization is responsible for investigating security incidents, to whom information should be reported, and who has the authority (and responsibility) to seek additional resources when needed. To the extent that one of the purposes for conducting an investigation is to provide in-house counsel with information needed to make legal recommendations, the plan should consider whether an organization desires the investigation to be conducted under the auspice of the attorney-client and attorney work product privileges. If so, the plan should make clear that the investigation is operating under the direction of counsel and the plan should provide instructions to the employees who may be collecting information concerning how to preserve privilege, including involving legal counsel in the investigation of certain types of security incidents. Tip: Be sure to designate a project manager to hold the team members accountable for their assigned tasks and to ensure that the investigation is proceeding quickly.

- **Internal Contact Information**. Many plans also include a quick reference guide naming the people within an organization who can help in the investigation of a security incident. This should include the incident response team member and their cell phone numbers, along with individuals who can serve as back-up support in the event a response team member is unavailable.

- **External Contact Information**. Many plans include a quick reference guide naming the people outside of an organization who can help in the investigation of a security incident, which may include contacts with law enforcement (*e.g.,* FBI and Secret Service), outside counsel, forensic investigators, call-center support, credit monitoring, public relations experts, etc. If the organization has a cyber-insurance policy, the approved vendors should be identified in the plan.

**Tip: If your organization operates in the European Union and is subject to the GDPR, the plan should include the name of the lead supervisory authority and the relevant information for reporting a breach, as breaches resulting in a risk to the rights and freedoms of individuals may need to be reported to the regulator within 72 hours after your organization becomes aware of it.**

- **Recordkeeping**. Plans typically explain the type of documents and records that should be kept concerning the investigation in order to permit in-house counsel to reconstruct when the organization knew certain pieces of information and when the organization took certain steps. Such reconstruction may be necessary in litigation or a regulatory investigation.

- **Post-Incident Reporting.** Many plans discuss how the organization will take information learned during an incident and incorporate that back into the organization's security program. This might include "lessons-learned" from how an incident was handled or ways to prevent an incident from occurring again. Under the GDPR, organizations are required to document an incident, its effects, and any remedial action taken. If the organization decided it was not a reportable breach, it should document the basis for that decision.

---

BCLP is working with clients to assess – and mitigate – risks by putting in place the policies, procedures, and protocols needed to address data security breach issues.

## MEET THE TEAM

**Linda C. Hsu**

Los Angeles

linda.hsu@bclplaw.com
+1 310 576 2192

---