BCLP. Client Intelligent

Insights

HOW SHOULD COMPANIES INVESTIGATE SECURITY INCIDENTS?

Jan 14, 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.

INVESTIGATING A SECURITY INCIDENT

The best way to investigate a security incident is to follow an incident response plan that was put in place before the incident occurred and that takes into consideration the specific needs and resources of an organization. If an organization does not have an incident response plan, the steps that follow outline best practices that take into account possible legal requirements and obligations. When deciding how to investigate a security incident, an organization should consider the following factors:

INCLUDE LEGAL COUNSEL AT THE INCEPTION OF THE INVESTIGATION

Once a data breach has been discovered, the organization should notify its in-house legal counsel. That person can determine whether the involvement of outside legal counsel specializing in data breach response is necessary. If the organization does not have in-house legal counsel, then outside counsel should be consulted and retained as early as possible.

A primary benefit of involving counsel early in an investigation is to allow counsel to help decide whether the remainder of the investigation should be conducted under the cloak of attorney-client

privilege. If counsel recommends that the investigation should be led by legal, as the information obtained is necessary in order for counsel to provide the organization with legal advice, any employees that take part in the investigation should be instructed to copy counsel on all internal communications concerning the cause and the scope of the breach or, when speaking to others, to clearly indicate that they are collecting information at the behest of counsel. For example, if information needs to be requested from IT or HR by email, the subject line of the email should preferably read "Attorney Client Communication: Information Requested By Counsel" to make sure that anyone who reads the email at a later time understands the context in which it was sent, the purpose for which the information was being collected, and the fact that the communication may be privileged and exempt from disclosure outside of the organization.

Tip: Vendors should be retained by legal counsel to work at their direction in order to assist with providing legal advice to the organization.

FORM A CORE TEAM OF PERSONNEL TO ATTEND TO THE BREACH

Effectively investigating a security incident often requires a team of personnel. This may include representatives from IT/IS, legal or risk management, operations, marketing & communications, and human resources (if the breach involves employee misconduct or employees' personally identifiable information). Ideally, the team will have been identified and trained on data breach response prior to any incident. One person should be designated to keep a log or running chronology of the investigation to enable the organization to reconstruct, if needed at a later time, what information the organization knew at what time. Personnel should take extreme care when documenting the investigation to only include factual assertions about the breach and to avoid creating a factually inaccurate record or a record with opinions that may be based on preliminary information.

CONTAIN THE BREACH AND PRESERVE EVIDENCE

When dealing with an electronic breach, it is important to preserve all evidence and isolate the source of the breach. An organization's IT department should be advised to identify the source of the breach and isolate the compromised systems from the network. The organization should take care not to destroy or alter evidence and to continue monitoring the system (e.g., unplug the affected system; do not restart it or turn it off).

If the organization's IT department has relatively little experience with investigating security incidents, do not necessarily assume that they will automatically preserve evidence or understand how evidence should be preserved. To the contrary, IT departments that have historically focused on business continuity or user-experience may inadvertently overlook the steps needed to preserve the chain-of-custody of evidence in an effort to try to remove suspected malware quickly or to restore the functionality of certain items. In-house counsel may need to explain the importance of forensically preserving evidence in order to further examine, at a later point, whether the incident was in fact a breach, and, if so, the extent of the breach, including whether personal or sensitive

data was accessed. In some instances, in-house counsel may need to help IT understand what it means to forensically preserve evidence, and to evaluate whether IT's methods for copying and logging data would be defensible before a regulator or in court.

RETAIN A THIRD-PARTY FORENSIC INVESTIGATOR

Many competent IT departments lack the expertise, hardware, software, or personnel to preserve evidence in a forensically sound manner or to thoroughly investigate a security incident. In such a situation, in-house counsel needs to be able to recognize the deficiency quickly and recommend that the organization utilize external resources to help collect and preserve electronic evidence and investigate the incident.

As discussed above, in-house counsel should consider whether the investigator should be retained through in-house counsel or outside counsel to preserve the right to claim that the investigation and all notes related to it are protected by attorney-client privilege and the work product doctrine. The investigator should be able to investigate the attack vector, decipher the scope of the breach—including what records were viewed or acquired and how many times the third party gained access to the system—and identify whether, and how, data left the organization's information technology environment. These functions are sometimes referred to within the data security community as identifying "infiltration," "aggregation," and "exfiltration." The investigator also may be able to help in-house counsel coordinate with law enforcement efforts to catch a perpetrator, although, unfortunately, in most instances the perpetrator will remain unidentified or be located outside of the jurisdiction of most U.S. law enforcement agencies.

When retaining a forensic investigator, it is important to remember they will be given access to your organization's networks and there is a high likelihood that, if a breach occurred, they may gain access to sensitive personal information as part of their investigation. As a result, you should review the agreement between the investigator and your organization carefully to make sure the investigator agrees to apply the security warranted for the type of information to which they may gain access, and provides appropriate indemnification for any data security lapses of its own. A best practice used by proactive organizations is to identify and retain a forensic investigator before a breach occurs. Doing so will ensure that the organization will be able to negotiate favorable terms and conditions in the retainer agreement before a crisis situation eliminates much of the organization's bargaining power.

Tip: If you are subject to the GDPR, you should consider having an investigator sign a data protection addendum governing the access to and use of personal data.

ASSIGN A CRISIS MANAGER

Incident response teams are usually comprised of personnel from a variety of backgrounds and representing a variety of internal resources and departments. Because the members of a response

team rarely have the same reporting structure, confusion about who has authority to convene an investigation, assign projects, or retain needed resources can lead to inefficiencies.

A pre-designated crisis manager that reports directly to, and has authority conferred from, senior management often facilitates the most efficient response. This person should work closely with legal counsel to ensure attorney-client privilege is maintained. This person should hold each incident response team member and outside vendor accountable for completing their assigned tasks timely and efficiently.

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.

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Linda C. Hsu

Los Angeles

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