LITIGATION MINUTE: CREATING AN INCIDENT RESPONSE PLAN

DATA BREACH SERIES: PART ONE OF THREE

Date: 10 May 2022

By: Claude-Étienne Armingaud, Tyler G. Anders, Desiree F. Moore

WHAT YOU NEED TO KNOW IN A MINUTE OR LESS

Reported incidents of data breaches have reached record levels over the last two years.[1] Given this reality, a data security incident response plan is no longer a luxury; it is a vital tool in every company's larger crisis management plan. A well-thought-out and thorough response plan can both significantly reduce the confusion that often follows a data security incident, and reduce the pitfalls that often lead to regulatory scrutiny, putative class actions in the United States, and the fairly recent “group actions” in the European Union.

In a minute or less, here are the essential components of a working incident response plan.

Key Roles and Responsibilities

An incident response plan must identify those individuals responsible for invoking the plan and leading the response to any data security incident. It should identify one person (or a cohort of people, such as a security incident response team) who is ultimately accountable for leading the response, as well as clearly defined roles and responsibilities for all other response team members.

Once a plan is crafted, tabletop exercises can crystalize team members' respective roles, hone the necessary skills to navigate an incident, and facilitate teamwork in the wake of an incident.

This section of the plan should also include key external resources, such as a detailed contact list for legal counsel, forensic investigators, and law enforcement, including FBI, DHS, and local police as may be warranted. Considering the often-constricted timeframes for breach notification requirements, best practices dictate having these external resources identified and known to the company in advance, saving valuable time during a crisis.

Assessment, Containment, and Eradication of the Data Security Incident

The plan should also contain definitions that will guide the company in assessing the nature and scope of the incident in the early hours once a potential incident is detected. For example, assessing whether the incident is due to an internal threat actor or an external threat actor, or whether it is a ransomware event or a business email compromise or otherwise, will be critical to an effective early response.

Once the threat is assessed, the plan should outline steps for containing the incident, including with the support of the key external resources noted above (such as counsel and a forensic firm).

Internal Information Technology teams, as identified in the roles and responsibilities section of the plan, coupled with counsel and forensics (the latter to be engaged by counsel so as to preserve privilege where possible), will

be key to any assessment and containment efforts. These teams will work together to more fully assess the nature and potential scope of the incident, as well as how to contain and mitigate damage.

Communications Plan

Finally, the plan should anticipate the need to communicate about the incident, both internally and externally. Communications to the C-suite and board are almost always required in the immediate aftermath of the incident (and the board and C-suite will likely be named as key contacts above). Depending on the incident, select or all employees may need to be informed. For example, a ransomware event impacting all email systems likely requires a communication to all employees. Legal counsel can assist with language for any such communication. This can be done in advance in the plan, with modifications to be made in the wake of an actual incident.

Legal counsel can also help determine the timing, scope, and content of any external communications as well, including to insurers, law enforcement, third-party vendors and/or business partners, and, depending on the incident, impacted data subjects and regulatory agencies as warranted or required by law. This section of the plan should therefore state when notifications may be appropriate, including the process for notifying key stakeholders and impacted parties in a timely fashion.

Lastly, the response team should discuss a "retrospective" of the documented incident to evaluate its cause and future preventative action. The incident response plan should be adjusted based on the lessons learned.

FOOTNOTES

[1] Experian Data Breach Resolution. (2021). *Eighth Annual Study: Is Your Company Ready for a Big Data Breach?* Ponemon Institute.

KEY CONTACTS

CLAUDE-ÉTIENNE ARMINGAUD
PARTNER

PARIS
+33.1.58.44.15.16
CLAUDE.ARMINGAUD@KLGATES.COM

TYLER G. ANDERS
ASSOCIATE

NASHVILLE
+1.615.514.1805
TYLER.ANDERS@KLGATES.COM

