BCLP. Client Intelligent

**Insights**

# NAVIGATING A SECURITY INCIDENT - BEST PRACTICES FOR ENGAGING SERVICE PROVIDERS

Sep 10, 2024

*With the recent wave of ransomware and other security incidents, it is now more important than ever for impacted organizations to have a thorough understanding of each element of a proper data breach response. That includes consideration of attorney-client privilege and work product issues when retaining third party consultants and vendors. Indeed, since the original publication of this guidance, at least one more court has seen fit to require a defendant in a lawsuit arising from a data breach to produce not only a forensic breach report but most communications with a forensic breach response firm, reasoning that the firm's work was sufficiently linked to business operations to require such discovery. See Leonard v. McMenamins Inc., No. C22-0094-KKE, 2023 WL 8447918 (W.D. Wash. Dec. 6, 2023). Caution in this area is warranted and the guidance below is as timely as ever.*

Organizations experiencing a security incident must grapple with numerous competing issues simultaneously, usually under a very tight timeframe and the pressure of significant business disruption. Engaging qualified service providers is often critical to successfully resolving and minimizing the fall-out of the incident. These providers include forensic firms, public relations firms, restoration experts, and notification and call center vendors. Due to the nature of these services, they can have access to or even generate additional personal and sensitive information relevant to the incident. Protecting this information from third party or unauthorized disclosures during litigation, discovery, or otherwise, via the application of attorney-client privilege and the work product doctrine[1] is essential.

While there is no bright-line, uniform rule about how and under what circumstances these privileges attach to forensic reports and other information prepared by incident response providers, recent case law offers guidance as to how organizations can maximize the prospect that their assessments will remain shielded by the work product doctrine and/or the attorney-client privilege. Below we identify a set of "Dos" and "Don'ts" to help organizations more effectively engage their service providers with these goals in mind. We recommend that companies incorporate these principles into their Incident Response Plan and distribute to the incident response team at the outset of every incident response effort.

## Engaging Incident Response Service Providers - Dos and Don'ts

- **DO** carefully structure the service provider engagement to establish a defined scope of work, separate payment process, and connection to future litigation concerns (as addressed in more detail below).
- **DO** delegate the engagement of service providers to external breach counsel (i.e., service providers should be engaged by external counsel on behalf of the organization and in anticipation of litigation).
- **DO NOT** engage the service provider directly. If external counsel is not involved, the Office of the General Counsel should engage the provider.
- **DO** use a separate contract or SOW for each security incident that includes a defined scope of services for the particular incident and specifies that the engagement is intended to assist breach counsel with its provision of legal advice in anticipation of litigation.
- **DO NOT** rely on existing MSAs with providers handling day-to-day business issues or providing services not specifically related to the current security incident (e.g., ongoing security monitoring services).
- **DO** categorize payments to incident response service providers as a legal expense.
- **DO NOT** categorize payments made to outside providers as a regular business expense.
- **DO** consider using a vendor with whom you do not already have an established business relationship (i.e., avoid using current IT vendor to perform forensic investigation), noting that this consideration will need to be balanced with other factors, such as the urgency surrounding the engagement, the financial and commercial terms of both existing and new arrangements, and the familiarity of an existing provider with company systems and/or the incident itself.
- **DO** clearly establish and utilize appropriate communication and reporting protocols with service provider teams.
- **DO** limit written communications concerning the incident and limit distribution to key stakeholders with a need-to-know.
- **DO NOT** engage in communications without the involvement or approval of counsel.
- **DO** have counsel (preferably external) manage the review, revisions, and distribution of reports prepared by providers.
- **DO NOT** receive reports directly from the service provider.

- **DO** consider bifurcating reporting to split factual reporting from recommendations and other subjective considerations, as facts are generally not subject to the attorney-client privilege.
- **DO** assume that reports (either in whole or in part) might be subject to disclosure at some point, such that there should always be a focus on well-drafted, streamlined, and accurate reporting.

As recent case law has shown, there is no absolute way to guarantee the protection of the reports and other information prepared by incident response service providers. However, following the above practices should enhance the prospects that the work product and attorney-client privileges will apply and withstand any motions to compel during litigation and discovery. Also, thinking early and often about the process will help minimize risk in the event that such information must ultimately be disclosed.

For more information about this issue as well as about how Bryan Cave Leighton Paisner LLP can help assist you with incident response, preparedness and defense, please contact Amy de La Lama, Christian Auty, or Daniel Rockey.

---

More information on communication “Dos” and “Don’ts” for incident response >

---

[1] The standard used to determine if the work product doctrine applies is whether the document was prepared in anticipation of litigation. A series of recent decisions from federal courts interprets this standard as precluding application of the privilege if the document would have been created in essentially the same form in the absence of litigation for business continuity or other non-litigation purposes.

## RELATED CAPABILITIES

- Data Privacy & Security

## MEET THE TEAM

**Amy de La Lama**

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

**Christian M. Auty**

Chicago

christian.auty@bclplaw.com
+1 312 602 5144

**Daniel T. Rockey**

San Francisco

daniel.rockey@bclplaw.com
+1 415 268 1986