Cybersecurity, Privacy & Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

Protecting Privilege: Top 10 Checklist for Cybersecurity Forensic Investigation Reports

September 18, 2020

Key Points:

- In ongoing multidistrict litigation concerning Capital One's 2019 data breach, Capital One succeeded in defeating a motion to compel disclosure of a privileged root cause analysis conducted by PwC.
- In contrast to an earlier ruling requiring Capital One to turn over a similar root cause analysis conducted by cybersecurity expert Mandiant, the court found that Capital One's general counsel engaged PwC through a distinct and legally privileged representation to assist the company with its fiduciary and legal duties in anticipation of litigation.
- As these rulings show, privilege determinations vary widely, but adhering to best practices can maximize the chance of avoiding disclosure.

On August 21, United States Magistrate Judge John F. Anderson of the Eastern District of Virginia sided with Capital One in a privilege dispute involving the company's 2019 data breach, finding that plaintiffs are not entitled to receive copies of a report that Capital One commissioned from PricewaterhouseCoopers (PwC) to analyze the technical and non-technical root causes of the breach. Plaintiffs had unsuccessfully argued that the report was not privileged because it served primarily a business, rather than a legal, need and that Capital One had waived any privilege by sharing copies with regulators, its auditor and more than 150 internal employees.

Ruling from the bench at a hearing on this issue, Magistrate Judge Anderson noted that the timing of PwC's retention was a key factor in his decision that the report was indeed privileged. Capital One's board and general counsel directly retained PwC after at least 60 lawsuits were filed in the wake of the data breach. In addition, PwC was retained expressly to advise the board on its fiduciary duties and to provide an independent expert opinion to Capital One's legal department as it established the company's strategy in defending against litigation and anticipated regulatory enforcement actions.

Importantly, Capital One took a number of steps to try to maintain privilege over the PwC report. Among them, the company shared the report only with those persons that

Contact Information

If you have any questions concerning this alert, please contact:

Natasha Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle Reed
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

Melissa Whitaker
Counsel
mwhitaker@akingump.com
Washington, D.C.
+1 202.887.4538

had a need to know the findings, including members of the board, the company's in-house legal department, senior executives with enterprise-wide responsibility for coordinating the company's response and members of the technology, cybersecurity and HR departments who played a role in remediation efforts. Distribution was further limited by restrictions prohibiting the majority of recipients from printing the document or otherwise sharing copies. Copies shared with regulators were provided only as required by law, while Capital One's auditor was permitted to view the report but not to have its own copy.

This decision comes on the heels of another privilege ruling in the same case in which the court ordered Capital One to produce a different root cause analysis written by forensic cybersecurity firm Mandiant. There, Capital One's pre-existing statement of work with Mandiant—which was drafted and agreed to prior to anticipation of any litigation—expressly contemplated that Mandiant would conduct a root cause analysis for the company in the event of a data breach. Although Capital One executed a new agreement with Mandiant after the 2019 data breach and claimed privilege over the resulting report, the court determined that there was no material difference in scope between the agreements and that the report was primarily for business purposes. In this case, even though Capital One and PwC had a pre-existing business relationship, Capital One did not have an agreement in place with PwC that contemplated performing a root cause analysis until after the first data breach lawsuits were filed.

These decisions highlight that across jurisdictions—and even within the same courtroom—maintaining privilege over a root cause analysis may come down to the thinnest of margins. Below, we offer some best practices to follow to maximize the chance of successfully asserting privilege over these reports.

Retain outside counsel to manage the investigation.

In the event of a data breach, retain outside counsel to conduct a legally privileged investigation. Whenever possible, outside counsel should directly engage the cybersecurity response vendor, even if a prior relationship between the company and the vendor exists. Work closely with counsel to document how the investigation will differ from other cybersecurity services the company regularly receives and explicitly include in any agreement that work will be undertaken at the direction of counsel.

Review preexisting agreements with cybersecurity vendors and establish separate statements of work specific to the breach.

Businesses with existing cybersecurity vendor relationships should review their current master services agreements to ensure that breach response work is kept separate from monitoring or other services. Revise prior agreements as needed with an eye toward refining potentially overbroad descriptions of the services to be rendered. If necessary, carve out work that the vendor is engaged to conduct specifically in anticipation of litigation, such as coordinating with outside counsel and performing technical analysis for benefit of the company's legal defense.

Avoid using stock language in the statement of work.

Simply copy-pasting the verbiage from a preexisting agreement with a cybersecurity vendor into a new agreement between counsel and the vendor does not automatically ensure the engagement is privileged. Consider your needs in anticipation of litigation and tailor the agreement language accordingly. This factor is critical to demonstrate

that any developed work product is created in a manner and form different from what would be created but for the anticipated litigation.

Think critically about requesting a written report of findings.

Companies should consider foregoing a written report of findings from the incident response vendor altogether. Findings and conclusions may be shared orally with key stakeholders.

If a written report is prepared, advise the preparers not to speculate while the preliminary investigation is ongoing. A written report that rests on conjecture and unsupported initial findings will not be helpful in future litigation. Unverified hypotheses should be conveyed orally and thoroughly investigated before they are documented as a “fact” or “finding.” Companies might also determine that they wish any written report to include a focus on exculpatory factors.

Create segmented teams to protect the privilege.

Responding to a data breach incident will likely require responses from multiple business units and external vendors, including teams focused on managing legal, regulatory, consumer, cybersecurity and governance aspects of the breach. To manage the response while protecting the privilege across these legal and non-legal groups, where possible, create segmented work streams assigned to distinct teams on a “need-to-know” basis. Engage outside counsel to direct the work of external vendors, including forensic analysts. The legal team may include members of in-house counsel, outside counsel and experts retained by counsel. Consider creating a separate email listserv to restrict access to information, calls and documents to the designated members on the legal team.

Limit distribution of privileged attorney work product.

Maintain the privileged nature of all attorney work product generated with regard to the incident and only share it as needed for litigation purposes, as opposed to business needs. Educate all team members on the importance of not forwarding communications or documents outside of the designated legal team and channeling incident-related communications through legal.

Keep track of where the written findings are shared and why.

If written findings must be shared outside of the legal team, document who receives the report and the reason for the distribution. If the need is a pure business need unrelated to preparing for litigation, avoid sharing the document in order to protect the privilege.

Prepare a separate, non-privileged incident report that can be shared.

After a data breach, information must often be disclosed to apprise board members, auditors, insurers and regulators. To meet these disclosure needs while protecting the privileged nature of the investigation, consider asking counsel to prepare a cover memorandum that addresses only non-privileged business needs and verified factual findings. This memorandum may be shared externally while protecting attorney-client privileged findings in a separate report prepared only for the use of counsel that may contain broader findings and conclusions.

Pay expenses from the Legal budget.

To the extent possible, fees related to any cybersecurity response overseen by outside counsel should come from the company's legal budget. While it may seem natural to deduct these expenses from the cybersecurity or IT budgets, some courts have focused on this factor as an indication of whether the company has consistently treated the response as legally privileged.

Be prepared for disclosure.

Court precedent on protecting privilege over forensic reports and/or work performed in response to breaches varies by jurisdiction and is constantly changing. Companies should prepare any written report with the understanding that the final report—as well as drafts, comments and edits to the report—may eventually be produced in litigation. For this reason, taking all necessary steps at the outset to address the incident properly and expediently will help ensure that, should information regarding the breach response ultimately be disclosed in litigation, it will not be to the company's detriment.

akingump.com