What's in your report? Disclosure of forensic reports after a data breach

Jun 03, 2020

Categories:

Blogs
Technology Blog

A federal district court in *In re: Capital One Customer Data Security Breach Litigation* recently held that the work product doctrine does not protect a cybersecurity consultant's report prepared after a data breach.

In 2015, Capital One engaged cybersecurity consultant Mandiant on a retainer basis for general data breach preparation. In 2019, Capital One proactively engaged Mandiant for a specific Statement of Work (SOW) for 285 hours of cybersecurity incident response support in the event a data breach occurred. The 2019 SOW provided that the consultant would provide a detailed final report covering the engagement activities, results, and recommendations for remediation if and when such a breach should occur.

Capital One experienced a data breach in March of 2019 and retained a law firm to provide legal advice in connection with the breach. The law firm immediately signed a Letter Agreement with Mandiant for Mandiant to provide services and advice regarding data breach response, forensics, incident remediation, and analysis. The agreement also specified that the agreed-upon services, including the report, would be provided to the law firm rather than the company.

A tide of litigation followed as soon as Capital One informed the public of the breach, which exposed the personal information of over 100 million people. Pursuant to the SOW and the Letter Agreement, Mandiant prepared a report discussing how the breach occurred and detailing the technical factors that allowed the criminal hacker to penetrate Capital One's systems. Mandiant sent the report directly to the law firm, which then provided it to Capital One's legal department, numerous employees, and the company's board, as well as four regulatory agencies and an accounting firm. There was no evidence that any copying or sharing restrictions were placed on the report.

The work product doctrine protects tangible work products prepared because of, or in anticipation of, litigation. The

determinative issue for the court was whether the report would have been prepared in substantially similar form but for the prospect of litigation. The "because of" standard is designed to protect only the work that was conducted because of litigation, not work that would have been done in any event or in the regular course of business.

The court ordered the release of the unredacted cybersecurity report after it found that Capital One could not satisfy its burden of showing how it would have investigated and reported the incident differently if there was no potential for litigation. The ruling was based purely on Capital One's failure to meet the "because of" standard. The court did not discuss any waiver arguments related to the broad disclosure to Capital One employees and other businesses and agencies.

Some of the factors that worked against Capital One in gaining work product doctrine protection for the report were:

- Capital One did not put forth any evidence that the report would not have been prepared but for this litigation.
- Capital One had a longstanding relationship and pre-existing agreements with Mandiant "to perform essentially the same services" that were performed for the report at issue.
- Capital One admitted that the agreement with Mandiant was to help it respond quickly to future incidents, implying that the report would have been prepared after a data breach regardless of whether litigation would occur.
- The court found it "significant" that Mandiant had already received a large retainer and agreed to perform 285 hours of work before the data breach was discovered.
- The report was provided to employees, other companies, agencies, the company's internal response team, and was used for compliance with regulatory requirements, which suggested it had regulatory and business reasons (rather than purely legal reasons).

Forensic reports of a data breach typically identify the likely method by which a threat actor accessed a company's IT environment, thus exposing critical vulnerabilities in its systems.

They may also identify areas in which a company failed to maintain industry standards or to maintain its contractual and fiduciary obligations to protect clients and employees' information. Undoubtedly, companies would want these reports to be protected to avoid having to hand them over to opponents during litigation. This case provides an important reminder that the fact that there is litigation does not, by itself, shield materials with work product immunity.

Here are some general guidelines that an organization can follow to strengthen the argument for protection against disclosure of forensic reports and related documents in litigation:

- Review and update the company's incident response plan to structure a breach investigation from the outset to prioritize the preservation of work product protection.
- Retain outside counsel to direct the scope of the forensic investigation to ensure any reports or conclusions are being conducted at the direction of counsel to provide legal advice or in anticipation of litigation.
- Limit internal distribution of reports and only disseminate to parties when consistent with the purposes of the attorney work product protection.
- Consider having dual investigations, with one team working on the business response and operational concerns, and another team directed by legal counsel to receive the information that will allow it to provide informed legal advice.

For questions and assistance regarding this topic, please feel free to contact any member of our Privacy and Data Security Team.

FBT Gibbons