Armstrong Teasdale

October 29, 2021 • Advisory • www.atllp.com

CYBERSECURITY INCIDENT REPORTS AND LESSONS LEARNED FROM RECENT COURT DECISIONS ORDERING THEIR DISCLOSURE

The rapid rise of cybersecurity incidents, and the litigation and government investigations that often ensue, have resulted in many hotly contested disputes concerning the disclosure of documents explaining 'what happened' and 'how.' In the past year, at least three courts have weighed in to resolve such disputes, each of which required disclosure.

In some cases, being ordered to disclose such documents can be problematic. Incident response reports, including those concerning forensic investigations and root cause analyses, can lay bare how and why certain systems were vulnerable to cyberattacks in the first place, potentially giving rise to or supporting claims of negligence and statutory violations.

The three recent decisions, however, also provide guidance on how available legal protections can be applied to incident reports.

APPLICABLE LEGAL PROTECTIONS

The *attorney-client privilege* (ACP) generally protects from disclosure information that is shared between attorneys and their clients for the primary purpose of obtaining or providing legal assistance. For assistance to be legal in nature, a lawyer must be attempting to guide a client's future conduct by interpreting and applying legal principles to specific facts.

The *attorney work product doctrine* (WPD) generally protects from disclosure documents prepared "in anticipation of litigation" by another party when there is identifiable or impending litigation that has been or is the "primary purpose behind the creation of the document."

In cases involving malicious attacks of Capital One, Clark Hill and Rutter's – a bank, law firm and convenience store chain – filed in Virginia, the District of Columbia and Pennsylvania, courts analyzed the application of ACP and/or WPD to cybersecurity incident reports.

PEOPLE
Jeffrey Schultz, CIPP/US

SERVICES AND INDUSTRIES
Data Innovation, Security and Privacy

THE TRILOGY

In re Capital One Consumer Data Security Breach Litigation

In July 2020, in one of many lawsuits filed against Capital One for a data breach that involved unauthorized access to information for over 100 million individuals, a Virginia court required Capital One to disclose an incident report prepared by outside counsel. In analyzing whether the report should be protected under the WPD, the court stated:

In order to be entitled to protection, a document must be prepared "because of" the prospect of litigation and the court must determine "the driving force behind the preparation of each requested document" in resolving a work product immunity question.

Applying this standard, the court believed the incident report would have been prepared anyway, even if the cybersecurity incident had not occurred because, among other things:

- The work performed for Capital One by its technical consultant prior to the data breach and then for Capital One's outside counsel after the data breach was the same.
- Capital One had treated the technical consultant's work as a business-critical expense. It was not converted to a legal expense until months after its outside counsel was retained.
- The incident report would have been prepared for regulatory purposes anyway – it was given to four regulators, an accountant and a senior vice president.
- The incident report also would have been prepared for business purposes. More than 50 Capital One employees were given the report, without explanation as to why.

Based on the above, the court determined that the WPD did not apply and ordered Capital One to turn the report over the plaintiffs.

Wengui v. Clark Hill, PLC

In January 2021, a Washington, D.C., court was asked to determine whether a law firm that experienced a cybersecurity incident should be required to disclose a forensic report. Since other purposes for the report existed – i.e., threat mitigation and advice relating to the configuration of its systems – the court said the report was not protected by the WPD.

The court also said that since the report was widely circulated – including to members of Clark Hill's leadership and IT teams, as well as the FBI – for a range of "non-litigation purposes," it must not have been prepared in anticipation of litigation. As a result, the court ordered the report be disclosed.

In re Rutter's Data Sec. Breach Litig.

In July 2021, a Pennsylvania court ordered disclosure of a report examining how a convenience store chain suffered a cyberattack to its point-of-sale machines (*In re Rutter's Data Sec. Breach Litig.*, 2021 U.S. Dist. LEXIS 761 (M.D. Pa. Jan. 2021)). Like *Capital One* and *Clark Hill,* the court in *Rutter's* found that the report was not protected by the ACP or the WPD. Specifically, the court found that the ACP and WPD did not apply because:

- The agreement between Rutter's counsel and the technical consultant did not sufficiently evidence that the report was in anticipation of litigation.
- Rutter's corporate designee testified that he was not anticipating any litigation as a result of the cyberattack and that the report would have been prepared anyway.
- The report's primary purpose was to set forth "facts;" it did not assert any legal opinions, principles or strategies relating to Rutter's legal exposure.

PROTECTING REPORTS UNDER ACP AND WPD

Organizations seeking to maintain ACP and WPD protection for reports generated in connection with a cybersecurity incident should consider the following:

- Engage counsel and clearly articulate that the work to be performed is in anticipation of litigation based on the industry, jurisdiction and information involved.
- Limit communications concerning the reports, including reports prepared at outside counsel's direction, to those involved with making decisions based on the legal advice provided.
- Withhold reports from other teams within an organization to better show that the purpose of the reports is to provide legal advice to in-house counsel and management.
- If a technical consultant engaged by outside counsel has a preexisting relationship with the affected organization, make sure there is a separate agreement for outside counsel's work.
- Ask outside counsel to communicate to technical consultants that they are being retained to assist outside counsel with providing legal advice based, in part, on the underlying facts.
- Outside counsel should clearly articulate that they are providing legal advice in relation to the facts so that that can they assess and understand the legal obligations potentially at issue in anticipation of litigation.

As the above cases demonstrate, maintaining ACP and WPD protection for all

reports generated by technical consultants may not be feasible. Companies should keep in mind that such reports may ultimately be discoverable. Armstrong Teasdale's Privacy and Data Security practice is actively monitoring relevant litigation in this space. Please contact your regular AT attorney or one of the authors below for additional information.