PROTECTING IT FORENSIC REPORTS IN THE WAKE OF A DATA BREACH

Hodgson Russ Cybersecurity & Privacy Alert
October 1, 2020

No company plans to be the target of cybercriminals. However, data breaches take place daily, compromising customer names, email addresses, passwords, credit card numbers, social security numbers and other sensitive information. According to the Identity Theft Resource Center there were 811 data breaches in 2019, and 540 through June of 2020. Companies like Walgreens, Estee Lauder, JCrew, MGM Resorts, T-Mobile, Marriott and Nintendo, were among the victims of these attacks in 2020. At times, it seems the odds of avoiding a data breach are stacked against us. In fact, an entire industry has developed around positioning businesses to immediately and deftly respond to any potential compromise of their computer system.

In the aftermath of a significant security incident, there are hundreds of decisions to be made amidst a chaotic environment and without the benefit of complete and accurate information. One of the most important decisions a business must make is whether and how to hire an IT forensic consulting firm. The conventional wisdom is that hiring an outside consultant is a critical step towards taking responsibility for, mitigating damage from and providing transparency into a security breach. And, as our experience bears out, hiring a consulting firm is indisputably the right approach in most cases. However, the process used to hire a consultant can have major consequences during a subsequent litigation or a government investigation.

Consulting firms invariably produce reports and form opinions about the nature, cause and scope of the breach. In many instances, the business will disclose all or a portion of the consultant's report to allay customer concerns, address regulatory inquiries and address other legitimate purposes. But, there are circumstances in which such disclosure may not be in the business' interest. For that reason, sophisticated companies retain legal counsel to oversee the post-breach analysis and response. Counsel, not the company, should normally retain the consultant to assist with the breach analysis and response. Until recently, well-settled judicial precedent, shielded attorney-supervised forensic reports as privileged and excluded them from disclosure in litigation. A recent decision from the U.S. District Court for the Eastern District of Virginia ("EDVA"), however, calls that principle into question.

Attorneys

Jane Bello Burke
William Ciszewski III
Alfonzo Cutaia
Reetuparna Dutta
Patrick Fitzsimmons
Michael Flanagan
Michelle Merola
Scott Paton
R. Kent Roberts
Gary Schober
Amy Walters

Practices & Industries

Cybersecurity & Privacy

PROTECTING IT FORENSIC REPORTS IN THE WAKE OF A DATA BREACH

On May 26, 2020, a U.S. District Court Magistrate Judge for EDVA, issued a decision directing Capital One to produce a post-breach forensic report prepared by Mandiant ("Mandiant Report"), a highly reputed IT consulting firm. Capital One argued that the Mandiant Report was work product prepared to help counsel develop its legal theories about the data breach and the strategy for defending the bank in litigation. The Court acknowledged the age-old rule that documents prepared because of the prospect of litigation are entitled to protection under the work product doctrine; however, it concluded that there was not sufficient evidence to demonstrate that the Mandiant Report was prepared to support litigation, rather than business purposes.

Specifically, the facts established that Capital One retained Mandiant in November 2015 under a Master Services Agreement (MSA) and thereafter entered into periodic Statements of Work (SOW). On January 7, 2019, Capital One paid Mandiant a retainer under a 2019 SOW which included incident response services. Capital One's accounting team designated the retainer as "Business Critical," not related to litigation or some other legal expense. On July 19, 2019, Capital One discovered a data breach that exposed significant Capital One customer information.

On July 20, 2019, Capital One hired the law firm Debevoise & Plimpton. Four days later, Capital One, Mandiant and Debevoise & Plimpton entered into an agreement for Mandiant's services, including "computer security incident response." The agreement stated that work would be done at the direction of counsel and that payment terms were the same as those set out in the 2019 SOW.

On July 29, 2019, Capital One issued a public announcement disclosing the breach and several lawsuits were filed the following day. In early September, Mandiant issued a report "detailing the technical factors that allowed the criminal hacker to penetrate Capital One's security." Mandiant's initial work was paid for through the January retainer and additional work was paid for directly by Capital One. Although the Mandiant Report was initially provided to counsel, it was subsequently sent to Capital One's legal department, Board of Directors, fifty Capital One employees, four regulators and an accounting firm.

The Court's legal analysis focused on the fact that Mandiant and Capital One had a pre-existing contractual relationship and that the same scope of services was effectively transferred to counsel. In addition, Capital One paid Mandiant first from its initial retainer and subsequently from its bank account, designating those fees as "business critical." The Court also noted that the Mandiant Report was used by Capital One for a variety of business and regulatory purposes. All of these factors compelled the Court's conclusion that there was a superficial transfer of the pre-existing relationship in an effort to shield the report from disclosure.

The Capital One decision is an important reminder to the business community that it is imperative to plan for the possibility of a data breach and, in doing so, to take the necessary precautions to protect the work product prepared in response to it. And although the Capitol One decision arises out of data breach incident in which litigation was anticipated, the same concerns can emerge for companies that seek legal advice about regulatory compliance. In either scenario, when hiring a consultant, the following best-practices should be observed in order to protect any subsequently-developed work product:

- Retain legal counsel ***before*** a consultant is hired.

- Legal counsel should retain a consultant with no pre-existing relationship with the business, if possible.
- The consultant's engagement agreement should be between counsel and the consultant only.
- The consultant should be paid by counsel and those fees should be included in the legal bills. This can be effectively managed by requiring the company to pay a retainer at the outset of the legal engagement which the lawyers pass on to the consultant.
- Counsel should define the scope of work to make clear that the work is being performed to assist counsel in the rendering of legal advice, i.e., the defense of a pending or anticipated litigation or for the purpose of complying with any applicable privacy and data security laws.
- ***Limit*** the distribution of any reports prepared by the consultant to those actually assisting with the legal matter. That includes individuals working on the litigation or those who need to have access for purposes of complying with any privacy and data security laws, including breach notification requirements. However, do not distribute reports to the entire internal information security and cyber teams, accountants, regulatory agencies or others with a business interest in the report.

The collaboration that exists between legal and forensics professionals is critical to a good outcome. But in the wake of a data breach, the exigencies of the moment can cause people to overlook how these relationships are structured.

For more information on preparing for and responding to data breaches contact Michelle Merola (518.736.2917), Gary Schober (716.848.1289) or Patrick Fitzsimmons (716.848.1710) to discuss how Hodgson Russ can assist.

If you received this alert from a third party or from visiting our website, and would like to be added to our Cybersecurity & Privacy alert mailing list or any other of our mailing lists, please visit us **HERE**.