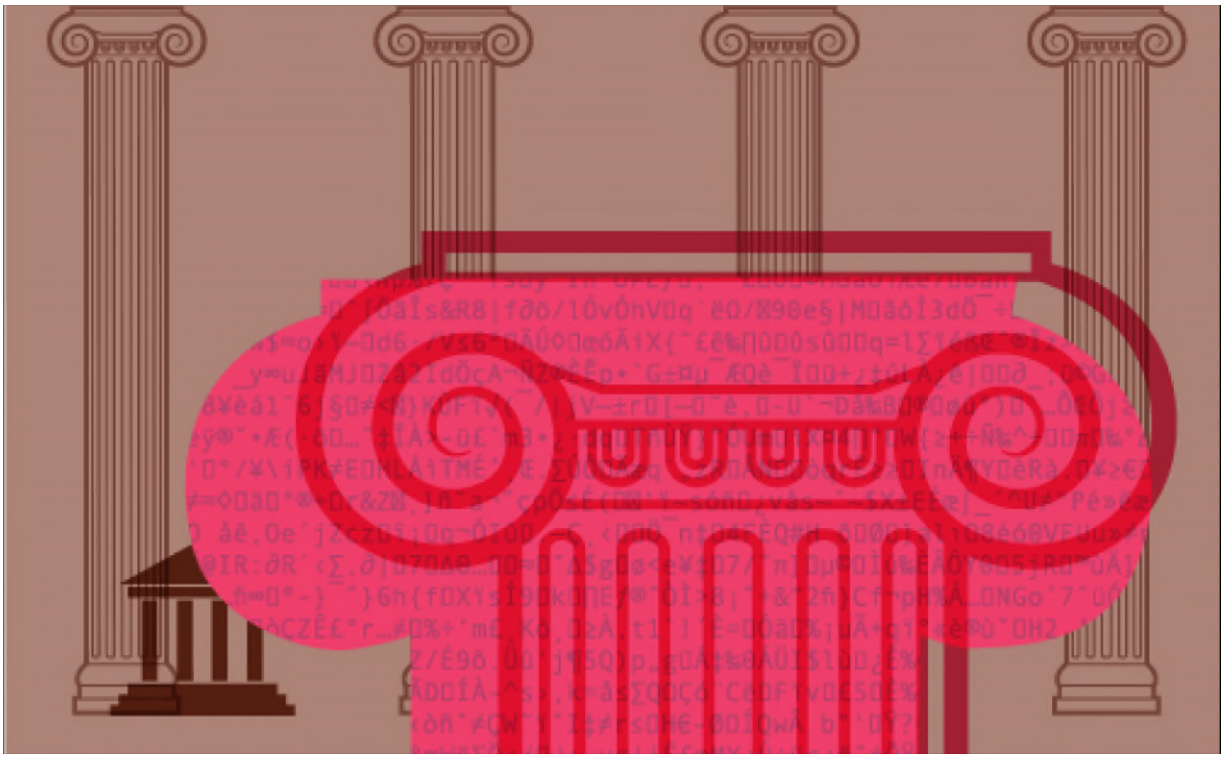
Protecting Privilege: Strategies to Keep Post-Cyber Breach Activities from Disclosure



By

Elissa Doroff and Melissa Ventrone

4/25/2016

Originally published in *Litigation Management* magazine, Spring 2016.

Today most businesses cannot avoid being, at least in some limited manner, connected to the information highway or having an online presence. As a result, the risk of experiencing a security incident or a data breach is a threat almost all organizations face. It seems every month brings another report of a high-profile data breach. For every mega-breach that is reported, numerous smaller breaches go unreported by the media.

Many organizations struggle with the question of how to handle a data breach appropriately, efficiently, and in a way that mitigates the harm to itself and its customers. In addition, organizations must take into account the fact that a data breach could result in litigation, regulatory scrutiny, and inquiries by attorneys general. Thus, organizations have a vested interest in protecting breach-related communications, documents, and actions taken.

Involving an attorney at the earliest opportunity after a breach is discovered - may provide protection pursuant to the attorney-client privilege and the work product doctrine to the data breach response process, limiting the reach of discovery down the road should litigation result.

Attorney-Client Privilege

Clearly, attorney-client privilege provides protection for communications between the client and attorney. When this privilege is applied to the attorney-client relationship, clients are more likely to be open and frank with their attorneys. This in turn enables the attorney to better service the client. Generally, for the attorney-client privilege to apply, the communication must be confidential and for the purpose of securing or obtaining legal advice. In the context of a data breach, information obtained during the investigation enables the attorney to render a legal opinion; but what about when a third party, such as a forensic investigator, is engaged to assist?

Mitigation of and response to a data breach often requires the assistance of a computer security or cybersecurity firm to conduct a forensic investigation. Unfortunately, many times organizations have not adequately thought through the response process, and the internal IT department may engage a forensic investigator directly. From the organization’s perspective, this may make sense as the IT department is likely more familiar with these types of companies and their qualifications and the investigation will require the cooperation of IT. Thus, from the organization’s perspective, why wouldn’t the IT department engage the forensic investigator?

Those opposed to involving legal counsel early in the response process may argue that the attorney-client privilege would not be applicable at this point as the forensic investigator would have been retained regardless of whether a lawsuit was filed. Under this theory, the forensic investigator would be viewed as providing a traditional business function outside the scope of the attorney-client privilege or the work product doctrine.

However, opponents of early attorney engagement fail to understand the many legal obligations with which an organization must comply after suffering a data breach — some of which require legal action within 48 hours of discovering the breach. Under the numerous federal and state data breach statutes, notification obligations are triggered when personally identifiable information (PII) is either accessed or acquired by an unauthorized individual. In those cases when a hacker attacks the system, how can an attorney opine on whether notification obligations have been triggered unless a forensic investigator reviews the evidence and determines how the attacker gained access to the system, whether any PII was at risk, and whether the hacker accessed or acquired the PII?

...Organizations should ensure that any engagement of third-party vendors in response to a data breach is done with legal counsel."

Even in those instances where the data breach occurred through human error rather than through an attack by a third party, the assistance of a forensic investigator may still be needed to provide the attorney with information necessary to determine whether notification obligations have been triggered. For example, consider an organization that creates a portal through which customers can register to pay their accounts online. After registering for the first time, the customer receives an email with a link to the new account. An enterprising customer subsequently informs the organization that the last four characters of the link can be altered such that the user can see account details for another customer. Forensics would be needed to determine how long the vulnerability was in place, how many individuals accessed the links, and what type of information may have been compromised. Legal counsel requires this information to render an opinion as to the organization's notification obligations.

The concept of attorney-client privilege applying to forensic investigations is supported by *Genesco, Inc. v. Visa U.S.A., Inc.,* which held that an outside consultant's investigation into a cyber attack was privileged where the consultant was retained by outside counsel in contemplation of litigation and to assist counsel in providing legal advice regarding a cyber attack.

Thus, organizations should ensure that any engagement of third-party vendors in response to a data breach is done with legal counsel. To further protect the privilege, the contract with the third-party vendor should include language that specifically states that the purpose of the engagement is to enable counsel to provide legal advice, including legal advice in anticipation of litigation and regulatory inquiries.

In addition, many organizations may have a cyber-liability insurance policy in place. Accordingly, consider whether an insurer may insist upon the insured providing the forensic report and why that may be necessary. First, forensic reports may be critical to understanding the facts that ultimately drive the coverage determination. Second, since the insureds almost always seek coverage for the costs of the forensic reports, it seems only reasonable that the insurer should have the right to review this information. Third, the insurer will need to assess the scope of work to determine whether the costs were reasonable and necessary. Finally, and most importantly, almost all cyber liability policies will provide contract language requiring that the insured cooperate by providing any and all documentation and information within their possession relative to the circumstance or claim. As such, there are very strong reasons for an insurer to insist on obtaining a copy of the forensic report absent an extraordinary reason in a particular case for the insured to withhold it.

Work Product Doctrine

In addition to the attorney-client privilege, documents created during the investigation should be protected by the work product doctrine under Federal Rule of Civil Procedure 26(b)(3).

"Ordinarily, a party may not discover documents and tangible things that are prepared in anticipation of litigation or for trial by or for another party or its representative (including the other party's attorney, consultant, surety, indemnitor, insurer, or agent)."

There are two types of work product — opinion work product and ordinary work product. While opinion work product consists of the opinions, mental impressions, or legal theories of an attorney or another party representative, ordinary work product consists of factual information that does not contain opinions or impressions. Ordinary work product may be discoverable if the opposing party can show that it has a substantial need for the materials and cannot, without undue hardship, obtain the information by other means.

Thus, some may argue that the work product doctrine does not apply to documents created during a data breach investigation as they were not prepared solely in anticipation of litigation, and these documents cannot be obtained by other means without undue hardship. However, the requesting party frequently can discover the underlying facts through depositions or other discovery methods. Documents prepared during or in response to the data breach investigation are created outside the normal course of business. Additionally, under *Simon v. G.D. Searle & Co. and United States v. Deloitte LLP,* work product protection will apply if litigation is one of the reasons for a document's creation, not necessarily the only one. If one of the primary purposes behind the internal investigation was to obtain or provide legal advice, the privilege will apply. For documents created during a data breach investigation, the work product doctrine can be a valuable tool to assist the organization with protecting the information from discovery.

In light of the many privilege concerns, organizations should tailor their incident response process to require the involvement of legal counsel as quickly as possible after learning of an incident. Counsel's involvement in the selection and retention of a forensic firm and other vendors could be the difference in a privilege dispute, and could prevent sensitive post-incident communications and documents from being made public.

About the Authors. . . .
Elissa Doroff is a Vice President and Product Manager for XL Catlin's Cyber and Technology Underwriting team. Melissa Ventrone is an attorney in Wilson Elser's Chicago office and chair of the firm's Data Privacy & Security practice.