UT LAW CLE THE UNIVERSITY OF TEXAS SCHOOL OF LAW

PRESENTED AT

2016 Essential Cybersecurity Law

August 19, 2016
Austin, Texas

Privilege Considerations in Cyber Incident Response

Bart Huffman

Privilege Considerations in Cyber Incident Response
by: Bart Huffman, Locke Lord LLP

As with other types of crisis situations, a cyber security incident can generate not only operational issues, but also significant legal exposure. Affected companies should think through the associated privilege issues, especially when consultants are used.

A company's response has a number of purposes: (a) containment, remediation, and continuity; (b) investigation and analysis to determine the cause and extent of the compromise; (c) internal and external communications and messaging; (d) compliance with legal requirements and regulatory expectations; and (e) preparation for the possibility of litigation or administrative proceeding. Various types of non-public written records may be created and used, such as:

- minutes of meetings;
- communications among the response team, with the employee base, with consultants, with potentially affected third parties, and with law enforcement;
- minutes of meetings;
- notes (e.g., generated during an investigation); and
- work papers and reports.

Some of these records may be privileged as attorney-client communications or protected under the work product doctrine. If litigation ensues and a consultant serves as a testifying or non-testifying expert, the consultant's work may be protected under the applicable procedural rules.

Applicable Contours of the Privilege

The attorney-client privilege protects communications made for the purpose of obtaining or providing legal advice. In *Upjohn Co. v. United States*, the U.S. Supreme Court held that communications by a company's employees to the company's legal counsel relating to an internal investigation, made for the purpose of securing legal advice, are protected by the attorney-client privilege. 449 U.S. 383, 386-87, 394-97 (1981). The work product doctrine protects an investigation or analytical work done at the direction of an attorney to prepare for litigation. *See* Fed. R. Civ. P. 26(b)(3); *Hickman v. Taylor*, 329 U.S. 495 (1947).

Courts have clarified that obtaining or providing legal advice need not be the *only* purpose for an investigation in order to maintain privilege. As applicable in the context of an internal investigation, it is sufficient if providing legal advice was "one of the significant purposes." *In re Kellogg Brown & Root, Inc*., 756 F.3d 754, 758 (D.C. Cir. 2014) (incorrect to presume that communication could have only one primary purpose). In other words, the fact that there are also business purposes to a post-breach investigation does not necessarily render the investigation (and

Also available as part of the eCourse
Essential Cybersecurity Preparedness and Response: Internal Controls, Developing an Incident Response Plan and Responding to a Data Breach.

First appeared as part of the conference materials for the
2016 Essential Cybersecurity Law session
"Responding to a Data Breach"