FOLEY

FOLEY & LARDNER LLP

CYBERSECURITY

Best Practices to Maintain Privilege Over a Post-Incident Forensic Report

After a cybersecurity incident, it is common to engage a computer forensics examiner to investigate the cause and scope of the incident. Because litigation commonly follows cybersecurity incidents, you may want to protect the forensic report under attorney-client and attorney-work product privilege. However, several recent court decisions have rejected privilege claims. Thus, it is critical to plan ahead and take steps to establish the privilege over the forensic report using the following best practices as your guide.

Establish an Incident Response Team

As part of your incident response plan, determine in advance who your incident response counsel and computer forensic examiner will be, and clear them beforehand with your cyber insurer. Incident response counsel should include attorneys engaged for the purpose of handling litigation, and those attorneys should work with the forensic team.

Use an Independent Forensic Provider

If your company uses an outside-managed security service provider, consider selecting a different computer forensic examiner for incident response purposes. Note that findings from an incumbent provider may be less objective, as the provider is unlikely to consider itself as having contributed to the incident.

Also consider excluding forensics and incident response services from the scope of your service provider agreement. Unless expressly excluded, incident response services could be viewed as in the ordinary course of business.

Engage Outside Counsel to Manage Incident Response

When an incident happens, engage outside counsel immediately. Outside counsel should retain your preferred computer forensic examiner and expressly state that the engagement is in anticipation of litigation and to assist in providing legal advice.

If outside counsel is engaging a forensic examiner with whom you have an existing relationship, ensure that a new service agreement or statement of work specific to the forensic investigation is used. Ensure that the forensic examiner interfaces with outside counsel rather than directly with your company. Outside counsel should define the scope and purpose of the investigation and be the first to receive the forensic report.

Avoid Using the Same Agreement for Business and Legal Purposes

If you have already engaged a computer forensic examiner in response to an incident, work with your outside counsel to document the work the examiner has done and shared thus far. Outside counsel should then enter into a separate agreement with the examiner with a modified scope following the abovementioned principles.

Consider Paying for Forensics from the Legal Budget

If a forensics examiner is being used to aid in the provision of legal advice, consider paying for such expenses out of the legal budget, rather than the IT or another departmental budget.

Maintain Confidentiality; Limit Distribution

Maintain confidentiality of the forensic report, limiting distribution to those who need to know and only disclosing redacted portions or summaries where possible. With the guidance of outside counsel, limit the distribution and disclosure of attorney-work product only where needed for anticipated litigation or legal advice.

Consider Whether a Written Report Is Necessary

Before a written report is prepared, consider, in consultation with counsel, whether requesting one is appropriate. The agreement with the forensic provider need not include a report as an engagement deliverable. Instead, consider noting that a written or oral report may be prepared and delivered upon the affirmative request of counsel.

Develop a Non-Privileged Report

Almost every incident either requires or would benefit from the sharing of information stemming from the forensic investigation. Various third parties, including board and management members, external auditors, customers, business partners, insurance adjusters, regulatory authorities—and plaintiffs in the event of litigation—are all parties that may seek access to information related to the incident.

Accordingly, counsel may be in the best position to create a second, non-privileged report shared with such parties. In contrast, the privileged report may include additional content that would be useful for providing legal advice.

Consider Limiting Forward-Looking Advice

Consider restricting or excluding forward-looking cybersecurity recommendations from the report, as these may not be considered legal advice. Further, consider the impact of including any recommendations that are ultimately not implemented by the company. Note, however, that privilege may still apply if the remediation measures are prescribed to assist outside counsel in preparing for litigation—e.g., by showing mitigation measures.

Always Consider the Possibility of Disclosure

While the forensic report and the attorney-work product prepared in anticipation of litigation is generally drafted with the expectation of remaining protected from disclosure, there is always the possibility of the report's disclosure. Consider the potential for discovery in litigation and be thoughtful when drafting the report—whether the final report, interim drafts, or commentary thereon.

Consider a Dual-Track Investigation

Depending on the circumstances, consider creating a dual-track investigation, with one track focusing on operations and the other focusing on legal. This may require retention of two separate forensic providers or two independent teams from the same provider. The operational team may be focused on investigating the source of the security incident and remediating its cause, working with the internal IT team.

In contrast, the legal track, retained by counsel, provides information directly to counsel to aid in providing legal advice to the company. This may help define the separation of privileged and non-privileged information. As noted, however, this is not the industry standard, nor should it be viewed as required to keep the privilege.

Engage Foreign Counsel for Cross-Border Incidents

Each jurisdiction and country have different rules and procedures for protecting attorney-client communications and work-product, in addition to other differences that may impact the legal considerations of a data incident in a given jurisdiction. Thus, local counsel would advise on how best to protect privilege in such jurisdictions.

Because this area of law is evolving, there is no way to guarantee the protection of the forensic report from discovery. However, following the above best practices will enhance the chances that the attorney-client and attorney-work product privilege withstand scrutiny.

For More Information

To learn more about this topic or discuss related best practices, please contact the following Foley attorneys or any Partner or Senior Counsel core member of our **Cybersecurity Practice**:

Matthew D. Krueger
Partner

Milwaukee | Washington, D.C.
414.297.4987
mkrueger@foley.com

Eileen R. Ridley
Partner

San Francisco | Los Angeles
415.438.6469
eridley@foley.com

Aaron K. Tantleff
Partner

Chicago
312.832.4367
atantleff@foley.com

Jennifer L. Urban
Partner

Milwaukee
414.297.5864
jurban@foley.com

For continuing coverage and additional industry insights, subscribe to Foley's Privacy, Cybersecurity & Technology Law Perspectives blog, which provides information and perspectives on the latest news and developments in privacy, cybersecurity, and technology impacting businesses in today's ever-connected world.