LJN LAW JOURNAL NEWSLETTERS

Cybersecurity LAW & STRATEGY®

An ALM Publication

June 2018

Protecting Privilege Before and After a Cyber Breach

Critical to any counsel working to prevent a cyber-attack or respond to a successful cyber intrusion is an understanding why and how to properly utilize both attorney-client and work-product privilege. The overriding principle of using privilege is straightforward: to protect your organization's investigation and breach response efforts from usage by third parties or regulatory agencies in litigation arising from a breach.

By Robert W. Anderson and Eric B. Levine

If you are not already thinking about cybersecurity for your company or firm, you should be. Regardless of your organization's size or industry, cyber crime is probably the greatest threat to your bottom line today.

One of the most important things a company/firm can do is to regularly conduct an investigation to understand what its cybersecurity defense weaknesses and vulnerabilities may be. The results of such an investigation most likely will produce a lengthy list of potential problem areas that in an ideal world should all be promptly and exhaustively remedied. Many times, this remedial approach is not feasible as most companies have budgetary and other practical limitations that may require them to prioritize which vulnerabilities to address first, and the degree of remediation of each such vulnerability that can reasonably be undertaken at a given time.

Unfortunately, another problem with this scenario is that the company or firm will end up with a written report identifying all variety of cybersecurity weaknesses, and then a set of actions that address some — but not all — of those weaknesses. If, at a later date, the organization experiences a cyber breach incident, this written report is likely to become Exhibit A of any plaintiff action against the company over that breach. The report, after all, shows that the company or firm clearly knew about certain vulnerabilities and chose not to remedy several of them.

Critical to any in-house counsel working to prevent a cyber-attack or respond to a successful cyber intrusion is an understanding of why and how to properly utilize both attorney-client and work-product privilege. The overriding principle of using privilege is straightforward: to protect your organization's investigation and breach response efforts from usage by third parties or regulatory agencies in litigation arising from a breach.

The Issue of Privilege

The attorney-client privilege protects confidential communications between attorneys and clients over the course of a professional relationship from discovery by adverse third parties. The work product doctrine protects from disclosure those documents and other tangible things that a party or a party's representative prepares in anticipation of litigation.

For their own protection, in-house attorneys should look to have their outside counsel attorneys make all arrangements necessary to employ the services of the proper outside consultants who will perform any cybersecurity vulnerability assessments and reports. If these vulnerability assessments are being undertaken at the direction of an attorney for the purpose of being able to provide legal advice to the

Robert W. Anderson and **Eric B. Levine** are partners with Lindabury, McCormick, Estabrook & Cooper, P.C., and co-chairs of the firm's Cybersecurity and Data Privacy practice. Based in Westfield, NJ, Lindabury serves clients throughout the Mid-Atlantic region.

attorney's client, then arguably the report detailing the client's long list of cybersecurity weaknesses will be protected from disclosure under attorney-client privilege. This can allow the company to be comfortable in doing the right thing by having its cybersecurity evaluated, and then undertaking reasonable steps to improve those cybersecurity protections — but potentially avoiding having that list of vulnerabilities turned over in a future plaintiff litigation.

Dangers for In-House Counsel

Companies with their own in-house counsel may sometimes want to avoid the additional expense of hiring outside counsel to arrange the cybersecurity vulnerability investigation. Having in-house counsel undertake the arrangements, however, may risk losing the attorney-client privilege. In-house counsel tend to have dual roles in the companies at which they work — often providing both general business advice as well as legal advice. It may therefore be more difficult for a company to prove that the in-house counsel was truly retaining the outside investigatory firm for the purpose of providing legal advice (rather than simply as part of the in-counsel's general business role at the company or as an officer of the company).

Outside counsel tend to be brought in specifically for the purpose of providing legal advice, and thus the potential dual role issues that in-house counsel are prone to can be avoided. In-house counsel should work closely with management at their company to evaluate when it is appropriate to bring in outside counsel in connection with a cybersecurity vulnerability investigation — and thereby potentially obtain the benefits of attorney-client privilege for the results of that investigation. The benefits can be substantial.

What to Do If There Is a Data Breach

Initially, while in-house counsel may have an attorney-client relationship with their companies, activities that are part of their daily job functions are potentially not going to be viewed by a judge as being taken explicitly to provide legal advice in anticipation of litigation arising from a cyber breach, thereby weakening any privilege argument. In other words, if in-house counsel is responsible for evaluating the operations of its company on a daily basis, the analyses performed and conclusions reached are more likely to be viewed by a court as part of a standard corporate function rather than action taken to provide legal advice or to defend against a distinct lawsuit.

In contrast, engaging outside counsel for the sole purpose of overseeing the company's data response team and breach response for the specific purpose of insuring proper operations provides a compelling argument in support of privilege. Outside counsel is being brought in for a narrow purpose (hopefully) and not on a regular basis but in response to a distinct event and with one specific objective, insuring the data breach response is properly performed to comply with the law and to reduce liability from any litigation commenced by those whose data has been accessed. Outside counsel reports are focused on minimizing the risks arising from the breach, and in today's environment related to data privacy, lawsuits following data breaches are virtually a certainty.

To cloak any data breach response under the umbrella of privilege, in-house counsel should contact outside counsel as soon as the breach is identified. The first call made by in-house counsel should be to its designated outside counsel member of the company's cyber breach response team. It should be outside counsel who engages the response vendor/data forensics specialist, on behalf of the affected company. All communications should run strictly between outside counsel and the vendor used for the breach response, including any report or findings of the vendor.

Once the breach is contained, outside counsel should meet with in-house counsel to review the findings of the vendor, to insure proper implementation of any remedial measures, and to follow outside counsel's recommendation putting into motion further steps to protect against litigation, such as issuing any proper breach notices to affected persons under the appropriate state laws, responding to any regulatory requirements, notifying insurance carriers and identifying witnesses and documents to be used at trial.

No business ever wants to have to face a serious cyber breach incident. Making proper use of the protections afforded by attorney-client privilege can be a crucial element of the plan to reduce the businesses' exposure to liability.

—❖—

LINDABURY
McCormick, Estabrook & Cooper, P.C.
Attorneys at Law

Robert Anderson
RAnderson@Lindabury.com | 908.233.6800

Eric Levine
ELevine@Lindabury.com | 908.233.6800