Reducing Insurers' And Insureds' Cyber Risks Through Strategic Teamwork

By Hillard Sterling

This article discusses challenges faced by counsel in helping insurers and clients to address and reduce their cyber risks and proposes specific and tangible measures to overcome those challenges.

The cybersecurity legal landscape is evolving, creating challenges for counsel in addressing clients' cyber risks. States are intensifying their activity and enacting laws setting standards of conduct for the protection of data. Agencies on the state and federal levels have issued – and will continue to issue – a panoply of regulations reaching across the spectrum of industries.

This intensified activity raises two central challenges that are front-and-center for cyber insurers and counsel advising clients about cyber risks. First, how do companies reach a defensible level of compliance? Cybersecurity compliance is easy to state conceptually, but a massive challenge to achieve in practice. Many companies are subject to a patchwork of state and federal laws, including regulatory guidelines, many of which may be inconsistent or in tension. This is particularly true in highly regulated industries including healthcare and financial services.

A second and directly related challenge is how to achieve defensible compliance without creating exhibits for adversaries. Cybersecurity is a massive undertaking that requires close participation and collaboration across a company, from the Board room to C-level leadership to the IT department. Everyone needs to communicate and work closely together to identify and address cyber risks. Yet in doing so, the participants create documents, hence potential evidence, much of which is invariably critical of the company's practices, historically and at present.

Those challenges, moreover, are present in any setting involving cyber risk. One such setting is the insurance-procurement process, in which insurance carriers must assess prospective insureds' cyber risks to determine whether to offer coverage, how much coverage to provide, and at what cost. This process is rife with risk, as insurers attempt to understand their prospective insureds' cybersecurity risks and exposure, and insureds respond with information about their cyber strengths and weaknesses. Typically, this occurs in the context of questionnaires submitted by insurers and answered by insureds, exploring the adequacy of the insureds' cybersecurity readiness. These questionnaires, however, vary in length and depth, and are not necessarily focused on specific measures required for legal compliance. Furthermore, the procurement process inevitably generates documents laden with admissions and negative information that are discoverable – and potentially devastating – in subsequent lawsuits and investigations.

Section I below briefly discusses the tangible and serious risks of creating non-privileged documents for use by prospective adversaries, including a well-publicized recent example illustrating these risks --- the Capital One decision, in which plaintiffs successfully pursued the production of a post-breach forensics report.

Section II identifies tangible measures for counsel to help address their challenges – compliance and confidentiality – through stronger collaboration with clients and insurers, i.e.: (A) Assembling a cybersecurity team focused on pursuing legal and technological compliance under the protections of the attorney-client communication privilege; (B) Structuring

Hillard Sterling is a partner at Clausen Miller P.C., where he is Chair of the firm's Technology and Cyber Group. Hillard has over 30 years of litigation experience defending technology companies against a wide range of technology claims, from systems-implementation disputes to data-breach cases. Hillard also counsels clients on developing and implementing best practices before, during, and after data breaches and incidents. In addition, Hillard assists insurers and insureds as a "breach coach" to quarterback data-breach responses and mitigation.

the cybersecurity plan and engagements to utilize the privilege; (C) Coordinating and managing risk assessments and additional cyber protections; (D) Reviewing and analyzing contracts with third parties that store or use data; and (E) Reviewing progress regularly and incorporating improvements.

To be sure, these measures will not stop plaintiffs from filing lawsuits or regulators from pursuing fines after a data breach. However, with strong compliance efforts and careful document management, exposure is reduced, making a legal or regulatory challenge less attractive. Cyber claims are easier to defend if counsel, insureds, and insurers have worked together to implement a focused and compliant cybersecurity program with appropriate privilege protections in place. After all, plaintiffs and regulators prefer low-hanging fruit, as a matter of simple economics, and may opt to forego a challenge if the potential payoff is lower and tougher to achieve. Eventually, stronger compliance should translate into additional positive benefits for insurers (hence their insureds) as underwriters evaluate lower risks and adjust premium prices downward.

Stop Writing Exhibits For Your Adversaries

When breaches occur (usually a "when" proposition, not an "if"), plaintiffs' lawyers and regulators target cybersecurity-related documents with laser-like intensity. There will be smoking (at least smoldering) guns, and companies need to run their cybersecurity programs while protecting the documents generated therein. Few companies are doing that properly, and even fewer companies structure their cybersecurity program with a central focus on the need to protect their information from subsequent disclosure.

This is not a hypothetical problem. Rather, it is playing out in courtrooms and agencies across the country, as plaintiffs' lawyers and regulators are demanding and securing detrimental and sometimes devastating evidence to support their allegations of cybersecurity deficiencies. Fueling these tactics, courts have been permissive in allowing data-breach lawsuits to proceed despite the absence of any cognizable damages suffered by plaintiffs, including massive class actions that are premised on the mere fact of a data breach, regardless of whether any class members actually suffered monetary harm.

The *Capital One* case is one well-known recent example of the risks raised by inadequately managed communications. *In re Cap. One Consumer Data Sec. Breach Litig.*, No. 1:19MD2915 (AJT/JFA), 2020 WL 2731238 (E.D. Va. May 26, 2020), aff'd, No. 1:19MD2915 (AJT/JFA), 2020 WL 3470261 (E.D. Va. June 25, 2020). In that case, a magistrate judge in the Eastern District of Virginia ordered the disclosure of a post-breach forensics report prepared by Mandiant. The judge held that the report was not protected by the attorney-client privilege, or the work-product doctrine, because it was not clearly undertaken for purposes of assisting counsel in the provision of legal advice or the defense of impending litigation. Rather, the report focused on the company's technological risks and business issues, not principally legal compliance.

Capital One raises a foreboding red flag about the discoverability of cybersecurity documentation. If plaintiffs may access *post-breach* forensics reports, despite their clear importance in assisting counsel, *pre-breach* documents certainly are fair game. The time-honored axiom holds true in cyber – everything you write can and will be used against you in a court of law – and it is counsel's job to get that message across loudly and clearly.

Implement A Compliant And Protective Cybersecurity Program

Counsel should undertake several categories of measures in order to navigate clients through potentially treacherous cyber waters, with compliance and privilege as guiding lights. All of these measures, discussed below, will enhance counsel's and their clients' efficacy in pursuing cyber compliance while minimizing the creation of potentially troublesome evidence. In addition, these measures will help counsel defend against post-breach claims and establish that clients' protective measures were compliant under applicable laws, regulations, and the ubiquitous standard of "reasonableness" required under multiple statutes and common law.

Assemble a Cybersecurity Team Focused on Compliance and Privilege

Know What "Compliant" Means for Your Client

Many companies structure their cybersecurity program so that they are led by technology executives, typically the Chief Information Officer (CIO) or Chief Information Security Officer (CISO), who identify and pursue protective measures based on technological priorities and costs. However, the CIO and CISO frequently do not communicate or coordinate with counsel, at least not until there is a legal problem or challenge. The result, unfortunately, is a failure to focus on achieving true legal compliance, or even understanding what legal compliance really means. Making matters worse, without counsel involved, the participants inevitably create documents that are ill-conceived and discoverable, exposing the company to enhanced risks of an adverse judgment or unfavorable settlement when a lawsuit or investigation erupts.

It is *counsel's* job to manage the cybersecurity team, not vice versa. And counsel's first job is to research and understand the law governing their clients' cybersecurity readiness. This is no easy task, yet it is absolutely necessary for counsel to guide the team towards true legal compliance. Companies, in fact, may be subject to multiple state laws, depending on where they do business and where their customers are located. Some states have expansive cybersecurity requirements, including California, New York, and Massachusetts, all of which have enacted comprehensive statutes, and issued expansive regulations, detailing specific mandates as well as vague requirements to implement "reasonable" cybersecurity measures. Counsel must know these laws and translate them into specific and tangible cybersecurity measures that are necessary for compliance.

Since there are many and varied legal standards across state lines (and between state and federal governments), many of which may be inconsistent, the safest compliance program aims to satisfy the

highest-common denominator. Counsel should identify and strive to comply with the applicable legal standard that is most stringent. Analyze the applicable state and federal law; identify the legal duties that would satisfy *them all*; and build the program to meet those duties.

Identify and Try to Achieve Safe Harbors

In addition, counsel must be focused on safe harbors that are available under various statutory regimes. These safe harbors often provide a legal defense against data-breach lawsuits if the breached company's program satisfies certain cybersecurity frameworks, such as those published by the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS). Other safe harbors are pegged to regulations issued under such statutes as HIPAA or Gramm-Leach Bliley. While these safe harbors are critical for counsel to know, and for companies to satisfy, they are sometimes vague (pegged to amorphous standards such as "reasonableness"), causing some harbors to be more treacherous than safe.

Companies need strong cybersecurity policies governing data access, transmission, storage, and use.

Structure the Team to Create and Protect the Privilege

Counsel should select their cybersecurity teammates with both compliance and privilege as the touchstones. The CIO and CISO, of course, are critical participants, as well as their teams who perform the difficult day-to-day tasks. However, some of these participants may pose dangers on the privilege front. Some states restrict the attorney-client privilege to communications between counsel and the "control group," typically defined as those with corporate decision-making authority. Illinois, for example, applies the "control group" test, and considers employees to be in the "control group" if "(1) the employee is in an advisory role to top management, such that the top management would normally not make a decision in the employee's particular area of expertise without the employee's advice or opinion; and (2) that opinion does in fact form the basis of the final decision by those with actual authority." *Archer Daniels Midland Co. v. Koppers Co.*, 138 Ill. App. 3d 276, 279 (1st Dist. 1985). While CIOs and CISOs should be part of the "control group" (if their decision-making authority and actions satisfy the above standards), other IT professionals may not be covered, including the CISO's team members and security specialists who typically do not report directly to other C-Level officers or the Board. Communications with those outside the "control group," therefore, need to be restricted and managed carefully.

Counsel also need to engage and work with third parties, including managed-service cybersecurity providers, which are critical components of any compliance cybersecurity program. Those are the teammates who are responsible for assessing and mitigating technological risks, to complement counsel's focus on legal risks.

Third-party engagements need to be structured strategically and carefully, starting with the engagement letters themselves. As an initial matter, counsel's engagement letter with their clients – the companies they serve – should make clear that counsel will be retaining a third-party cybersecurity vendor to assist counsel in the provision of legal advice. Then counsel should draft the engagement letter with the cybersecurity vendor to make abundantly clear that the vendor's services are focused on the same purpose – assisting counsel in the provision of legal advice – which is the foundation of the attorney-client privilege as a matter of black-letter law.

It is necessary, but not sufficient, to execute strong engagement letters setting forth the predicate for the attorney-client communication privilege. Counsel also should develop and implement a communication plan to detail the proper flow of communications – who should communicate with whom, and in what manner, so as to maximize the strength of prospective privilege claims. The communication plan, though, is only effective if the team members *know* and *follow* it. Training is critical here, and counsel should hold initial and periodic meetings with the cybersecurity team to educate and inform the team about the importance and logistics of proper communication flow.

Manage Risk Assessments and Other Cybersecurity Measures as Your Client's "Cyber Quarterback"

Risk Assessments

Risk assessments are one of the initial, and most important, components of any robust cybersecurity program. Companies cannot address their cyber risks without knowing and understanding their vulnerabilities, and risk assessments are their mechanism for doing so. Risk assessments also are critical for insurance carriers, who need to understand their prospective insureds' potential exposure, which drives the determination as to whether to offer a cyber policy, which risks to cover, and the terms and conditions of the coverage.

Some insurance carriers, in fact, bake the risk assessments into their underwriting and procurement processes. Many of those carriers require risk assessments as a condition of coverage, and others require risk assessments in effect (if not expressly) by requiring their prospective insureds to complete risk questionnaires that include the elements of a formal assessment.

While the importance of risk assessments is an accepted fact (or, at least, it should be), the best practices for undertaking those assessments are less known and followed. Whether required by insurance carriers or done outside of the insurance context, many companies initiate risk assessments internally, without the involvement of counsel, thereby ensuring that the assessments are vulnerable to disclosure to plaintiffs' lawyers or regulators. Worse, also discoverable are the myriad documents generated during the course of risk assessments, including emails, meeting notes, and texts, many of which are filled with negative information and admissions that become inculpatory

(sometimes devastating) evidence in the hands of an adverse lawyer or regulator.

Risk assessments, in short, are absolutely essential for insurers and their insureds, yet they also are potentially devastating weaponry when placed in the wrong adversarial hands.

Accordingly, counsel needs to spearhead the risk-assessment process, just like the larger cybersecurity program in which the assessments play a vital part. As referenced above, counsel should engage the cybersecurity vendor selected to undertake the assessment, and the engagement letter needs strong language to memorialize the predicate of the attorney-client privilege – *i.e.*, that the assessments are undertaken to assist counsel in the provision of legal advice.

Also, the cybersecurity vendor should communicate directly with counsel during the risk-assessment process. As a practical matter, of course, not all communications should (or can) be run through counsel. However, counsel's communication plan should ensure that the key communications – including the issuance of the report itself – are directed to counsel. The plan also needs to ensure that the documents generated by the assessment – again, including the ultimate report – are restricted to the corporate "control group," as defined by governing state law, so that the cybersecurity vendors and the companies do not inadvertently waive the privilege.

Additional Cyber-Protection Measures

Policies and Training

Risk assessments are necessary but not sufficient components of a strong cybersecurity program. There are multiple additional components that counsel should quarterback. Companies need strong cybersecurity policies governing data access, transmission, storage, and use. These policies should not be cookie-cutter, but instead tailored to the companies' specific data needs and risks. Although the substance of these policies should be unique to each company, they cover similar areas that are risks to every company, including standards governing email, passwords, remote use, mobile devices and smartphones, and social media.

Incident-Response Plans

Every cybersecurity program also needs to incorporate incident-response plans, which govern the processes for addressing breaches, and table-top exercises, which test those plans in realistic breach simulations. Most companies are doing both, but frequently not well, especially if these plans and table-tops are undertaken without the close involvement and assistance of counsel. If companies are creating incident-response plans on their own, and testing them without counsel present, they may be causing more harm than good, since plaintiffs' lawyers and regulators may access those plans and exercises to bolster lawsuits and investigations.

Best Practices

Counsel also should advise their clients (carriers or insureds) on implementing best practices that reduce cyber risks.

These practices may be industry-specific, particularly in highly regulated industries such as healthcare, manufacturing, or financial services. Healthcare providers, for example, should consider implementing cybersecurity measures recommended by the Healthcare Information and Management Systems Society (HIMSS). Financial institutions should understand and incorporate measures proposed by the Federal Financial Institutions Examination Council (FFIEC). Other best practices apply regardless of the industry in which the companies operate, including the need for strong encryption (for both transferred and stored data), firewalls, identity and access management (IAM), cloud use and storage, and threat detection. CIOs and CISOs are critical participants here, since they are the technologists versed in the best practices (and their respective costs and benefits) but leaving that advice to those officers alone ensures that their statements will be accessed and exploited by plaintiffs' lawyers and regulators interested in leveraging alleged shortcomings.

Review and Analyze Contracts with Third Parties Hosting or Holding Data

It is counsel's job, as part and parcel of a strong cybersecurity program, to review (and, when possible, negotiate) contracts with third parties whose actions (and inactions) create cyber risk. Companies increasingly are turning to the cloud to store their data, given the perceived benefits in cost and security. Counsel should review any existing cloud contracts to identify and react to potential areas of risk. Since those contracts usually are drafted by the cloud vendors, they likely have limited warranties, exclusive remedies, damages limitations, indemnification restrictions, and other provisions that implicate (and likely raise) cyber risks. While re-negotiating these deals may be difficult, cloud storage is a competitive market, and there may be opportunities to amend contracts in key areas, or perhaps even terminate contracts and move to another provider with more balanced provisions.

Cloud providers constitute just one type of third party whose contracts implicate cyber risks. Companies may be transferring data to business partners or advisors, to vendors who perform services related to the data (such as analytics or data mining), or a host of other third parties who access and/or use data as part of their operations. Counsel should analyze those contracts as well, or perhaps negotiate or re-negotiate them if feasible, to enhance protections and reduce risks, particularly in connection with warranties, damages, and indemnification provisions.

Revisit and Improve the Program

Like most everything in life, cybersecurity programs are imperfect. Even in the strongest and best-managed programs, there are unexpected challenges, sometimes because the technologies do not perform as expected, or more frequently, because human beings make mistakes. The strongest firewalls, for example, cannot prevent an employee from clicking on a phishing email and opening the door for malware and data exfiltration.

Given these realities, cybersecurity programs are evolving processes that change and adjust as challenges arise. Counsel should institute regular cybersecurity-team meetings, certainly at least monthly, to review progress, discuss challenges, and identify and incorporate updates and improvements. With counsel orchestrating these meetings, the information generated therein should be privileged, if appropriate protections were created and implemented.

Conclusion

The bottom line is that counsel plays an indispensable role in identifying cyber risks, developing compliance programs, and managing those programs to utilize the protections of the attorney-client communication privilege. Compliance advice is the responsibility of an attorney, not a technology officer, and there can be no attorney-client privilege unless counsel establishes protective measures and manages communications effectively. Those realities are palpable in all contexts in which cyber risks are present, from the procurement of cyber insurance to the initiation of a cybersecurity program, through every facet of business operations involving legally protected data, to potentially defending against a regulatory investigation or litigation regarding a data breach or other cyber risk.