"Do You Want to Know a Secret?"

Courts and Agencies Unwittingly Join Hackers in Exposing Secret Information

MEGAN BROWN, ENBAR TOLEDANO, AND TATIANA SAINATI

Megan Brown and Tatiana Sainati are partners, and Enbar Toledano is of counsel, at Wiley Rein LLP, Washington, D.C.

In November 2020, a group of hackers backed by the Chinese state exploited vulnerabilities in Microsoft Exchange software to hijack tens of thousands of corporate servers around the world in the Microsoft Hafnium cyberattack.

The incident was far from isolated. As anyone with an online presence is no doubt aware—if only from the inundation of "your data may have been breached" notifications—cybercrime continues to vex consumers, companies, and governments. In the United States, data breaches have increased nearly tenfold over the past two decades, leaving extensive damage in their wake. Among other effects, data breaches expose personal information, compromise sensitive business and governmental data, sow fear and uncertainty in online institutions, and inflict hundreds of millions of dollars in monetary damages. Cyberattacks are generating more and more litigation and regulatory oversight, which is stressing the traditional attorney-client privilege and exposing victims to increased risk.

Efforts by the Securities and Exchange Commission (SEC) to obtain information from the law firm and cybercrime victim, Covington & Burling serve as a dramatic example of how cyberattacks are threatening the boundaries of the privilege. The SEC's approach stands in marked contrast to how the federal government has historically dealt with cybercrime victims, but it is by no means an isolated example of the ways in which litigation and oversight surrounding data breaches are reshaping privilege law.

In this article, we review the federal government's traditional approach to cybersecurity and related information sharing, discuss the SEC's abrupt departure from that approach (in investigative tactics and by rule), and offer a guide to the growing body of case law marking the contours of the attorney-client privilege in civil litigation arising from a cyber incident. The bottom line is that the SEC poses a real and present danger to companies' "secrets," and savvy litigators must understand how cybercrimes can change the contours of the attorney-client relationship.

First Principles

Data breaches have many victims. The primary victim of a cyberattack is, of course, the entity whose systems or data were targeted and perhaps breached. It is that entity the hackers identified to try to exploit, and it is that entity the federal government traditionally looks to protect, including through confidential details about incidents reported to the Federal Bureau of Investigation (FBI), the U.S. Secret Service, and the Department of Homeland Security (DHS). But cyberattacks have other victims, too—the indirect victims like users, customers, employees, and business partners of the infiltrated entity.

Published in *Litigation,* Volume 50, Number 2, Winter 2024.

In recent years, civil litigation and government enforcement actions have threatened to erode the protections historically afforded to hacking victims. The federal government for years took the position that hacking victims must be protected by robust confidentiality regimes—including protection from premature public disclosure, immunity from government retribution, and absolute attorney-client confidentiality. The FBI has long touted its commitment to protect corporate victims, shielding victim identities in press releases and complaints, to encourage voluntary collaboration.

The SEC recently rocked the legal world with heavy-handed investigative tactics that appear to revictimize Covington & Burling after the firm voluntarily reported a cyberattack. The SEC sought to pierce the normally sacrosanct attorney-client relationship in the wake of the law firm's data breach, to explore whether any law firm clients were affected and may have failed to make disclosures. The agency took the position that the victim of a cyberattack—Covington & Burling—should be required to disclose information about, and the identities of, almost 200 clients in case those *clients* needed to be investigated for possible securities violations. The legal industry and corporations united in opposition to the SEC's tactics—to no avail.

In considering the SEC's motion to compel Covington to respond to a subpoena, the court reasoned, in effect, that it could not consider the broader impacts of the SEC's actions on cyber policy because its role was limited to assessing whether the SEC complied with the legal standards governing the propriety of a subpoena:

> The court understands and appreciates the policy concerns raised by Covington and amici. They are not unfounded. *The SEC's approach here could cause companies who experience cyberattacks to think twice before seeking legal advice from outside counsel.* See Chamber of Commerce Br. at 9–10. *Law firms, too, very well might hesitate to report cyberattacks to avoid scrutiny of their clients.* See Law Firms Br. at 9–12. The court's role, however, is limited. Its task is only to assess whether the subpoena exceeds the SEC's statutory authority or fails to meet minimum constitutional requirements. It is not to pass on the wisdom of the SEC's investigative approach.

Securities and Exchange Commission v. Covington & Burling LLP, 2023 U.S. Dist. LEXIS 127205, (D.D.C. July 24, 2023)

As discussed below, the outcome of this dispute should serve as a warning to the legal industry.

The SEC's aggressive approach comes at the same time as the SEC's decision in its new cybersecurity rules to upset the consensus of states, federal agencies, and Congress that victims of cyberattacks should not be required to publicly disclose cyber incidents before an incident is contained and before investigations have concluded. In contrast to that long-standing and coherent federal policy, the SEC recently adopted a final rule that requires public companies to disclose a material cybersecurity incident within four business days—a requirement that pressures companies to make disclosures with insufficient information and that risks revictimization of cyber victims.

The SEC's recent high-profile attack on the attorney-client privilege is concerning, but it is not the only potential threat to the attorney-client relationship. More often, the boundaries of the attorney-client privilege have been tested in civil litigation between hacking victims and their users or customers. In the wake of a data breach, downstream victims frequently join together to seek relief from the hacked entity that housed their data. Anticipating the potential for such litigation, cybercrime victims commonly engage both legal and technical experts to guide their post-breach investigation and response. Because those efforts are made in anticipation of litigation—and are frequently spearheaded by lawyers—hacking victims may expect the results of their investigations to remain privileged. But, in resolving discovery disputes, courts have not always agreed. Below, we address a few recent developments that should grab the attention of cyber advisers and litigators.

Illustration by Ellice Weaver

The Federal Government Has Traditionally Protected Cyber Victims

The federal government's approach to cybersecurity, and specifically to cybersecurity-related information sharing with the private sector, has evolved over time. But throughout, the government has generally prioritized victims' confidentiality both to protect organizations from revictimization and to encourage voluntary information sharing about events. As noted above, the FBI has protected cyber victims. FBI Director Christopher Wray explained the rationale behind this approach in a speech to the Detroit Economic Club on March 22, 2022:

> [W]e need what the private sector sees to protect companies, schools, universities, of all kinds. If American businesses don't report attacks and intrusions, we won't know about most of them, which means we can't help you recover, and we don't know to stop the next attack, whether that's another against you or a new attack on one of your partners. We like to say that the best way to protect one business is to hear from others, and the best way to protect others is to hear from that one.

Recognizing the importance of information sharing, relevant laws have traditionally had built-in protections that respected victims' legal privileges and that limited the use of information they shared with federal officials.

Way back in 2013, in response to "[r]epeated cyber intrusions into critical infrastructure," President Obama issued Executive Order 13636, Improving Critical Infrastructure Cybersecurity. The order was intended to create "a partnership with the owners and operators of critical infrastructure" by increasing "the volume, timeliness, and quality of cyber threat information shared with U.S. private sector entities so that these entities may better protect and defend themselves against cyber threats." To that end, the order specifically elevated "business confidentiality, privacy, and civil liberties."

Two years later, the executive branch expanded and refined its objectives. Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing, reiterated that information sharing between industry and the government "must be conducted in a manner that protects the privacy and civil liberties of individuals," "preserves business confidentiality," and "safeguards the information being shared," while nevertheless enabling the government "to detect, investigate, prevent, and respond to cyber threats. . . ."

The same year, Congress enacted the Cybersecurity Information Sharing Act of 2015, the product of years of consideration and careful compromise that was intended to encourage information sharing by cybercrime victims. Like the executive orders, the act sought to encourage private companies to voluntarily share cybersecurity threat indicators and other useful information with DHS by providing robust protections for disclosed information. 6 U.S.C. § 1504(d)(2)–(3). These protections included specific safeguards for attorney-client privileged information and a prohibition on the government's use of disclosed information for regulatory purposes, including enforcement actions. 6 U.S.C. § 1504(d)(5)(D)(i). In adopting these protections, the act aimed to foster a culture of trust and transparency among companies, industries, and government agencies, especially DHS and the FBI, and largely succeeded in doing so.

The SEC's attempt to pierce the attorney-client privilege threatens considerable harm.

Congress again reiterated those priorities in 2022, when it enacted landmark legislation directing DHS to develop new reporting requirements for cyber incidents affecting critical infrastructure. Like their predecessors, the new measures placed continued emphasis on confidentiality for shared information, protection from public disclosure, prohibitions on the use of shared information by the government to regulate or conduct enforcement actions, and—importantly—a clear preservation of the attorney-client privilege. *See* 6 U.S.C. § 681e(a)(5)(A).

These guide rails do more than incentivize effective information sharing. They also reinforce the importance of handling security vulnerabilities discreetly. The premature public disclosure of a hack can—and often does—lead to revictimization because details of a cyber breach can become a road map for renewed attacks. Hasty disclosures can also lead to the spread of misinformation at a time when companies, investors, and the public feel particularly exposed.

But this uniform policy of fostering trust, and promoting cooperation, between the public and private sectors through thoughtful confidentiality rules may be cracking. The same year that Congress instructed DHS to create new reporting requirements that would specifically uphold the government's focus on confidentiality, the SEC proposed a sweeping public disclosure rule that threatens to undermine federal policy and the incentives the government has created for victims to work with the government.

The SEC's New Cyber Rules Take a Bite Out of Confidentiality

On July 26, 2023, the SEC adopted a final rule requiring public companies to disclose "material" cybersecurity incidents within four days and to reveal their cybersecurity risk management, strategy, and governance—potentially providing a step-by-step guide for hackers to circumvent the protections these companies put in place.

Unsurprisingly, the rule has generated considerable controversy. In his capacity as the ranking member of the Senate Committee on Homeland Security and Governmental Affairs, Senator Rob Portman warned that the rule allows cybercriminals to damage national cybersecurity, impede law enforcement investigations, and hamper the government's responses to cyberattacks—all at a time when such attacks are on the rise.

As adopted, the rule potentially requires companies to disclose sensitive information about the response to ongoing attacks. The four-day period to disclose a material incident may force companies to provide information prematurely, hindering deterrence and recovery actions, investigations into attribution, remediation efforts, and outreach to other potential targets. It also exposes victims to additional attacks as hackers and copycats can pile on to try to exploit uncontained vulnerabilities or claim to have exfiltrated data to extort ransom payments.

The SEC's rulemaking did not grapple with the possible impact of early disclosure on privileged investigations. Nor did it offer a meaningful way to delay disclosures while victims work with the FBI or other law enforcement in investigations.

After much public pressure and pleas for delay from the entire American economy, the SEC agreed to two exceedingly narrow exceptions to the four-day reporting requirement: one exception applies if the U.S. attorney general provides written notice to the SEC that the disclosure poses a substantial risk to national security or public safety; the other allows companies subject to the Federal Communications Commission's notification rule to wait until seven days after alerting the Secret Service and FBI of such a breach. The new rule is devoid of the sort of protections for privilege contained in the Cybersecurity Information Sharing Act of 2015 and ignores pleas to delay reporting while containment and investigative activities proceed.

Remarkably, the SEC acknowledged that its rule "could potentially increase the vulnerability of registrants and the risk of future attacks," but the SEC predicted that the alleged value of rapid cyber incident disclosure to investors will outweigh the security risk to victims, the government, and the broader public.

The rule thus undermines the core of federal policy on addressing cybercrime—the understanding that "the best way to protect one business is to hear from others, and the best way to protect others is to hear from that one"—by eroding the liability, privacy, privilege, and use protections on information sharing that have long served to foster trust between the public and private sectors.

Since proposing its sweeping rule, the SEC has gone on to target one of the most fundamental principles underlying our legal system—the attorney-client privilege.

The SEC Targeted Covington and Its Clients

The law firm Covington & Burling, based in Washington, D.C., was among the victims of the Hafnium cyberattack in 2020. The hackers breached Covington's networks, gaining unauthorized access to private information about 298 publicly traded companies.

Covington investigated the incident and, laudably, voluntarily cooperated with the FBI. In its internal investigation, Covington determined that the hackers' target had been information related to China-focused policy issues in anticipation of the incoming Biden administration—an unsurprising focus, given the Hafnium group's ties to the Chinese state.

The SEC responded to Covington's internal investigation with its own investigation and a broad subpoena. In relevant part, after the firm protested and tried to protect is clients, the SEC sought the names of Covington's clients whose files were potentially affected by the breach. According to the agency, the SEC sought this information to determine whether any trading in the affected companies may have been based on material nonpublic information obtained in the cyberattack and whether the affected clients had made all the necessary post-incident disclosures. Covington refused to identify its potentially affected clients on grounds of privilege and client confidentiality.

The dispute went before the U.S. District Court for the District of Columbia. In support of its refusal to recognize Covington's assertion of the attorney-client privilege, the SEC argued that "Covington is regularly in possession of [material nonpublic information], the theft of which puts investors at significant risk. Neither Covington's position as a victim of a cyberattack, nor the fact that it is a law firm, insulate it from the commission's legitimate investigative responsibilities."

For its part, Covington vigorously challenged the SEC's approach, arguing that the SEC's action "is an unwarranted attempt to intrude on client confidences and the attorney-client privilege, the protection of which is a fundamental ethical obligation of the legal profession."

Dozens of law firms backed Covington and signed an amicus brief asserting that the attorney-client privilege should bar the disclosure of the client information sought by the SEC. These firms, including Covington's competitors, argue that the SEC is attempting to "breach well-established principles of confidentiality in the service of a fishing expedition" and "would turn attorneys into witnesses against their own clients." The U.S.

Chamber of Commerce also filed a brief opposing the agency's heavy-handed tactics, urging the court to consider the conflict between the SEC's tactics and the long-standing federal policies described above.

The federal judge in that case recognized the dangers of the SEC's tactics, observing that "the SEC's approach here could cause companies who experience cyberattacks to think twice before seeking legal advice from outside counsel." And "law firms, too, very well might hesitate to report cyberattacks to avoid scrutiny of their clients." This is a damning assessment of the SEC's approach. Unfortunately, despite these credible concerns, the court found its hands tied by the legal standard for enforcing a subpoena, though it substantially limited the agency to compelling the names of only seven of the nearly 300 clients that it targeted. Further proceedings may in the future revisit or refine these issues.

The Privilege at Stake Is Vital

The attorney-client privilege is the oldest privilege recognized in the common law. It exists to encourage full and frank communication between attorneys and clients and thereby promote the public interest in the administration of justice. The privilege "rests on the need for the advocate and counselor to know all that relates to the client's reasons for seeking representation if the professional mission is to be carried out." *Upjohn Co. v. United States*, 449 U.S. 677 (1981).

> Critically, the results of the consultant's investigation should be shared with the legal team alone.

To preserve the privilege, the Supreme Court has long recognized the importance of clear boundaries. "An uncertain privilege, or one which purports to be certain but results in widely varying applications by the courts, is little better than no privilege at all." Accordingly, the privilege protects communications, even if it would be "more convenient" for the government to get notes or information directly from attorneys.

The SEC's attempt to pierce the attorney-client privilege threatens considerable harm. Knowing that their discussions with counsel may not be protected, clients would likely withhold relevant information. Armed with incomplete knowledge, attorneys, in turn, may render ineffective representations. And companies whose law firms are swept into the government's investigatory dragnet would likely need to sue their own counsel to enjoin the disclosure of what has always been privileged information.

In the cyber context, these concerns would almost certainly result in companies deferring legal consultation after a cyberattack for fear of government retribution and premature public disclosure. But deterring businesses in the midst of a cyberattack from timely getting the help they need plainly weakens the private sector's cyber resilience. It would also undermine the culture of trust and transparency that the government has so carefully cultivated over 10 years to maximize the country's defenses against cybercrime.

Cyberattack victims rely on counsel for every strategic decision. Lawyers routinely oversee a company's cyberattack investigation and internal response, draft appropriate disclosures to government agencies and affected parties, ensure compliance with regulatory and other reporting obligations, evaluate liabilities and manage resulting litigation, and cooperate with government agencies to bring the hackers to justice. These manifold responsibilities require a complete mastery of the facts. And clients who believe that their attorneys may be forced to turn over relevant information will likely self-censor, thereby gutting the representation and the privilege designed to protect it.

Some Courts Also Threaten to Erode the Privilege

The SEC's targeting of Covington represents a dramatic and high-profile attack on the attorney-client privilege—one that will hopefully prove short-lived—but the SEC's subpoena of Covington's client records is not the only threat to the privilege posed by cyberattacks.

Cyberattacks often result in civil litigation. Individuals and business partners whose information was compromised may seek compensation from the company whose network was breached. In the ensuing dispute, parties have an opportunity to engage in discovery, which often entails inquiries into the cause of the cyberattack, the victim's prior awareness of and response to technological vulnerabilities, the universe of affected data and parties, and steps undertaken in the aftermath to close security gaps.

In responding to such discovery requests, there is (generally) no dispute that attorney-client communications are privileged from production. But what about communications that involve a third-party consultant?

In addition to lawyers, the response team following a cyberattack may include technical consultants, who are engaged to investigate how the attack occurred, what information was targeted,

and how to prevent similar attacks in the future. Because these third-party consultants are retained in anticipation of litigation (after all, doesn't every cyberattack pose a risk of litigation?) and may even report directly to the victim's attorneys, the common response to discovery requests for their work product and communications is to assert that they are privileged. But cyberattack victims have been unpleasantly surprised to find their privilege assertions rejected in court.

In addressing such disputes, courts have reasoned that the primary *and presumptive* reason to investigate a cyberattack is not legal; rather, it is business-oriented. In other words, courts have found that companies need to determine the cause of a cyberattack as an ordinary business function, regardless of whether litigation ensues. Because attorney-client and work-product privileges apply only to documents created primarily for legal purposes, their protections do not apply to these materials—even if they are created under the supervision of outside counsel and labeled as privileged.

But companies can take steps to protect efforts undertaken by third-party consultants at the direction of counsel to investigate and respond to cybercrime.

How Can Victims Maximize Their Protections?

While federal agencies and courts may be poised to erode the protection of the attorney-client privilege, lawyers and clients can take steps to protect themselves. The results of litigation over cyberattack privileges offer a road map for how protections could and should be enforced. In particular, many courts have determined that a cyberattack victim can undertake a two-track investigation. One track, the "business" track, aims to determine the cause of a cyberattack and how to remediate it; this track is not protected. A second track, the "legal" track, separately investigates the cyberattack for the purpose of educating counsel about any resulting vulnerabilities. The key to keeping the latter track within applicable privileges is its focus on providing counsel with the information needed to advise and defend the company in any potential litigation or regulatory or enforcement proceeding.

So how can a company ensure that its *legal* investigation is protected? Companies can take several steps.

First, and foremost, a legal investigation requires an independent statement of work. Frequently, companies have existing relationships with consultants for day-to-day work. When a breach occurs, companies will generally turn to these same consultants to investigate. But it is vital to distinguish between the consultants' (likely unprivileged) routine work and the (possibly privileged) incident response. A critical factor in establishing this distinction is the preparation of an appropriate statement of work. Simply updating an existing agreement or executing a separate work statement will not suffice. A statement of work covering an incident response must meaningfully delineate between a consultant's typical duties and those undertaken after a cyberattack at the direction of counsel.

Such a statement should clarify that the consultant has been engaged at the direction of counsel, that the consultant will assist counsel in understanding the incident, that materials produced by the consultant will not be shared beyond the legal team, and that the work is not related to ordinary remediation efforts—such as determining, in the first instance, how a cyber incident occurred and how to mitigate it. Rather, the consultant's legal investigation must relate to legal services: preparing for potential litigation or administrative inquiries.

Critically, the results of the consultant's investigation should be shared with the legal team alone. Investigative reports shared with business units or information technology personnel—even at the highest levels of the corporate structure—are less likely to qualify for the privilege. Courts have thus declined to extend the privilege to investigations whose results were shared with leadership and information security teams, but have upheld applicable privileges when readership was limited to in-house counsel.

In the event litigation or an administrative inquiry ensues, companies should also appropriately document their two-track approach. For example, any hold notice should clarify from the outset that the company has undertaken a separate legal investigation, that the results of that investigation were not shared—and are not to be shared—with any business units, and that the goal of the investigation was to prepare for and respond to any potential legal liability. In this way, later assertions of privilege are not only limited to discovery objections but are also borne out by company documents.

Companies can also conduct privilege trainings to ensure that all relevant personnel are aware of the distinction between a corporate investigation, conducted in the ordinary course of business, and a lawyer-driven investigation designed to respond to the legal threat posed by cyber incidents.

Conclusion

The exponential increase in cybercrimes reverberates across society and our legal system. Courts, regulators, policymakers, industry leaders, and attorneys all are learning how to navigate the novel risks posed by cyberattacks. Preserving the sacrosanct nature of the attorney-client privilege to foster unencumbered communications between victims of cyberattacks, their legal advisers, and government regulators is one critical component to building cyber resilience. ■