Harvard Journal of Law & Technology
Volume 36, Number 2 Spring 2023

HOW PRIVILEGE UNDERMINES CYBERSECURITY

Daniel Schwarcz, Josephine Wolff** & Daniel W. Woods****

ABSTRACT

In recent years, cyberattacks have cost firms countless billions of dollars, undermined consumer privacy, distorted world geopolitics, and even resulted in death and bodily harm. Rapidly accelerating cyberattacks have not, however, been bad news for many lawyers. On the contrary, lawyers that specialize in coordinating all elements of victims' incident-response efforts are increasingly in demand. Lawyers' dominant role in cyber-incident response is driven in part by their purported capacity to ensure that information produced during the breach response process remains confidential, particularly in any subsequent lawsuit. By interposing themselves between their clients and any third-party consultants involved in incident response, lawyers can often shield any materials produced after a breach from discovery under either attorney-client privilege or work-product immunity. Moreover, by limiting and shaping the documentation produced by breached firms' personnel and third-party consultants in the wake of a cyberattack, attorneys can limit the availability of potentially damaging information to plaintiffs' attorneys, regulators, or media, even if their attorney-client privilege and work-product immunity arguments falter.

Relying on over sixty interviews with a broad range of actors in the cybersecurity landscape — including lawyers, forensic investigators, insurers, and regulators — this Article shows how, in their efforts to preserve the confidentiality of incident-response efforts, lawyers may undermine the long-term cybersecurity of both their clients and society more broadly. We find that lawyers often direct forensic providers to refrain from making recommendations to clients about how to enhance their cyber defenses, restrict direct communications between cybersecurity firms and clients, insist upon hiring cybersecurity firms with

---

* Fredrikson & Byron Professor of Law, University of Minnesota Law School.

** Associate Professor of Cyber Security and Policy, The Fletcher School at Tufts University.

*** Lecturer in Cyber Security, University of Edinburgh School of Informatics.

For helpful comments and suggestions, we thank Matthew Bodie, Rainer Böhme, danah boyd, Jim Graves, Gus Hurwitz, Orin Kerr, Jeff Kosseff, Susan Landau, Jon Lee, Jamie MacColl, Bill McGeveran, Sasha Romanosky, Alan Rozenshtein, Jayshree Sarathy, Andy Sellars, Shauhin Talesh, Paul Vaaler, as well as participants in panels at the Privacy Law Scholars Conference, the Cybersecurity Law and Policy Scholars Conference, the University of Minnesota's Squaretable Series, the University of Cambridge's Security Seminar Series, and the FIRST Conference on Computer Security Incident Handling. Kaylyn Stanek provided superb research assistance for the Article.

limited familiarity with the client's networks or internal processes, and strictly limit dissemination of the cybersecurity firm's conclusions to the client's internal personnel. To ensure their clients do not inadvertently waive any legal confidentiality protections, lawyers also frequently refuse to share any written documentation regarding a breach with third parties like insurers, regulators, and law enforcement. Even worse, we find that law firms overseeing breach investigations increasingly instruct cybersecurity firms not to craft any final report regarding a breach whatsoever.

These practices, we find, may impair the ability of breached firms to learn from cybersecurity incidents and implement long-term remediation measures. Furthermore, such efforts to protect confidentiality inhibit insurers' capacity to understand the efficacy of different security countermeasures and regulators' power to investigate cybersecurity incidents. To reverse these trends, the Article suggests that materials produced during incident response should be entitled to confidentiality protections that are untethered from the provision of legal services. But such protections should be coupled with new requirements that firms impacted by a cyberattack disclose specific forensic evidence and analysis. By disentangling the incident-response process from the production of information that can hold firms accountable for failing to take appropriate and required precautions, the Article aims to remove barriers to effective incident response while preserving incentives for firms to take cybersecurity seriously.

TABLE OF CONTENTS

I. INTRODUCTION

In recent years, attacks on the computer systems of corporations, nonprofits, government agencies, and even individuals have accelerated at an alarming rate.[1] These cyberattacks have not only cost victims countless billions of dollars,[2] but have also undermined consumer privacy,[3] distorted world geopolitics,[4] and even resulted in death and bodily harm.[5] Efforts to prevent or mitigate the consequences of such cyberattacks abound; potential victims spend massive sums attempting to harden their computer systems and insure against the possibility that these defensive efforts will fail,[6] while governments at every level

1. DANIEL J. SOLOVE & WOODROW HARTZOG, BREACHED: WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT 17–34 (2022); Jeffrey L. Vagle, *Cybersecurity and Moral Hazard*, 23 STAN. TECH. L. REV. 71, 75 (2020).

2. *See* Jay P. Kesan & Carol M. Hayes, *Liability for Data Injuries*, 2019 U. ILL. L. REV. 295, 320 (2019); Sasha Romanosky, *Examining the Costs and Causes of Cyber Incidents*, 2 J. CYBERSECURITY 121, 129–33 (2016).

3. *See, e.g.*, William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1136 (2019); Derek E. Bambauer, *Privacy Versus Security*, 103 J. CRIM. L. & CRIMINOLOGY 667, 668 (2013); Daniel Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 738, 747–53 (2018); Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 243 (2007).

4. *See* Daniel Abebe, *Cyberwar, International Politics, and Institutional Design*, 83 U. CHI. L. REV. 1, 4 (2016); Rebecca Crootoff, *International Cybertorts: Expanding State Accountability in Cyberspace*, 103 CORNELL L. REV. 565, 568–71 (2018); Kristen Eichensehr, *The Law and Politics of Cyberattack Attribution*, 67 UCLA L. REV. 520, 523–25 (2020).

5. *See* Kenneth Abraham & Daniel Schwarcz, *Courting Disaster: The Underappreciated Risk of a Cyber-Insurance Catastrophe*, 27 CONN. INS. L.J. 1, 12–17 (2021); Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CALIF. L. REV. 513, 515 (2015).

6. *See* Charlotte Tschider, *Locking Down 'Reasonable' Cybersecurity Duty*, YALE L. & POL'Y REV. (forthcoming 2023) (manuscript at 5) (on file with author); Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985, 995 (2018).

implement policies designed to promote cybersecurity.[7] And yet, the risk of cyberattacks only continues to climb.[8]

The rising risks of cyberattacks have not, however, been bad news for many lawyers. On the contrary, lawyers who specialize in assisting firms that have experienced a potential cyberattack are increasingly in demand.[9] These lawyers — many of whom market themselves as "breach coaches"[10] — coordinate all elements of victimized firms' cyber-incident response, including directing internal firm personnel, retaining a third-party cybersecurity firm, managing public messaging, and communicating with insurers and government regulators.[11]

Lawyers' pole position in coordinating cyber-incident response is hardly inevitable. Even the most sophisticated lawyers are almost never technical experts in cybersecurity.[12] Moreover, while cyberattacks that jeopardize individuals' personal data can indeed raise significant legal questions under state breach notification laws,[13] many cyberattacks —

---

7. *See* Jeff Kosseff, *Hacking Cybersecurity Law*, 2020 U. ILL. L. REV. 811, 812; Susanna Bagdasarova, *Brave New World: Challenges in International Cybersecurity Strategy and the Need for Centralized Governance*, 119 PENN ST. L. REV. 1005, 1009 (2015).

8. *See* SOLOVE & HARTZOG, *supra* note 1, at 17–34.

9. *See* Daniel Schwarcz, Josephine Wolff & Daniel Woods, *Do the Legal Rules Governing the Confidentiality of Cyber Incident Response Undermine Cybersecurity?*, LAWFARE (Jan. 5, 2022, 8:01 AM), https://www.lawfareblog.com/do-legal-rules-governing-confidentiality-cyber-incident-response-undermine-cybersecurity [https://perma.cc/YZE4-7FPG].

10. *Id.*

11. More than 4,000 cyber-incidents in 2018 were coordinated by lawyers. *See* ADVISEN, ADVISEN'S CYBER GUIDE: THE ULTIMATE GUIDE TO CYBER SERVICE PROVIDERS 196 (2019), https://www.advisenltd.com/2019-Cyber-Guide-Survey [https://perma.cc/W2GL-74K7]. Similarly, the cybersecurity firm Crowdstrike reports that forty-nine percent of its investigations were directed by outside counsel in 2020. *See* CROWDSTRIKE, CROWDSTRIKE SERVICES CYBER FRONT LINES REPORT 15 (2020), https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeServicesCyberFrontLines.pdf [https://perma.cc/QH6P-C2TG]. This approach is accepted so widely that in-house attorneys explicitly recommend it in their professional publications. *See, e.g.*, Stephen E. Reynolds & Tiffany S. Kim, *Not to Fear, the Feds Are Here: Preserving Attorney–Client Privilege in Data Breach Response*, IN-HOUSE DEF. Q., Winter 2020, at 6.

12. One forensic investigator explained:

> If I'm dealing with an IT person [at a breached firm], I can understand what happened. I can engage with them and pick up minor details. But lawyers don't have technical background and often don't understand technical details. I did an investigation for a firm, and the corporate counsel was a real estate attorney who had no idea about [payment card industry] standards and was there to protect the brand. They simply didn't understand what's going on.

Zoom Interview with Forensic Investigator 6, (Jan. 4, 2022).

13. Mark Verstraete & Tal Zarsky, *Optimizing Breach Notification*, 2021 U. ILL. L. REV. 803, 809–39 (listing examples of legal issues under state breach notification laws). To be sure, cyberattacks often raise a range of legal complexities beyond a firm's notification requirements. Some, such as the scope of potential criminal liability for attackers, need not be resolved by lawyers hired by the breached firm. *See generally* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596 (2003). Others, such as whether the breached firm violated duties to customers or other third parties, may need to be assessed by a breached firm, though often it will not be necessary to do so until a potential lawsuit emerges. *See generally* Daniel J. Solove &

including the ransomware attacks that now predominate[14] — do not necessarily trigger these legal complexities.[15] Firms that experience a cyber incident nonetheless routinely employ lawyers to coordinate all elements of their response, even though firms victimized by noncyber incidents typically only hire lawyers when they need assistance resolving specific legal questions or are on notice of a potential lawsuit.[16]

Lawyers' dominant role in cyber-incident response is driven in part by their purported capacity to ensure that information produced during the breach response process remains confidential, particularly in any subsequent lawsuit.[17] Attorneys are uniquely able to provide this protection by interposing themselves between a client and any third-party consultants involved in incident response, including cyber forensic firms. Under long-standing caselaw, communications between such third-party consultants and the attorneys who hire them to help provide legal advice to a client are covered by the attorney-client privilege.[18] Additionally, any documents and mental processes of third-party consultants, such as cybersecurity professionals, are shielded from discovery under work-product immunity if they were produced in reasonable anticipation of litigation.[19]

Preserving confidentiality in this way has long been understood as vital for breached firms. In part, this is because the earliest cybersecurity breaches that firms were required to publicly report typically involved the compromise of individuals' personal information.[20] Legal costs and settlement fees are often some of the largest costs associated with these breaches, and insurers therefore prioritized minimizing the risk of litigation by involving lawyers in the incident-response process early on — a priority that later carried over to other types of incidents,

---

Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 587 (2014). This is especially true given how indeterminate and underdeveloped the law is in this arena. *See* McGeveran, *supra* note 3, at 1144; Justin Hurwitz, *Cyberensuring Security*, 49 CONN. L. REV. 1495, 1508 (2017).

14. *See* Tom Baker & Anja Shortland, *The Government Behind Insurance Governance: Lessons for Ransomware*, 2023 REGUL. & GOVERNANCE (forthcoming 2023) (manuscript at 1), https://onlinelibrary.wiley.com/doi/epdf/10.1111/rego.12505 [https://perma.cc/U9SX-YN4Z].

15. Ransomware attacks can implicate breach notification laws when personal information is accessed, though the relevant laws vary by state. For example, a victim can be subjected to a "double ransom" in which adversaries threaten to leak stolen data, in addition to encrypting data on the victim's systems. *See* SOLOVE & HARTZOG, *supra* note 1, at 41–43.

16. In large part, this is a byproduct of how ordinary liability insurance products function. Standard Commercial General Liability policies typically require insured firms to provide notice of an "occurrence" — meaning an accident or repeated exposure to harmful conditions — only when such an occurrence "may result in a claim." *See* INS. SERVS. OFF., COMMERCIAL GENERAL LIABILITY COVERAGE FORM 11 (2012). Even then, a general liability insurer will typically not appoint a lawyer for the insured until it is sued.

17. *See infra* Part III.

18. *See* United States v. Kovel, 296 F.2d 918, 922–23 (2d Cir. 1961).

19. *See* FED. R. CIV. P. 26(b)(3)(A).

20. *See* SOLOVE & HARTZOG, *supra* note 1, at 17–34.

such as ransomware attacks, where litigation was less common and legal fees represented a smaller portion of overall remediation and recovery costs.[21] A second reason that confidentiality concerns loom large in the wake of a breach is that state breach notification laws only require firms to disclose limited information.[22] Therefore, successfully avoiding disclosure in other legal processes may shield firms from disclosure's reputational and regulatory consequences. Yet another, more cynical, explanation is that the importance of confidentiality in the incident-response process helps the lawyers who dominate this process retain their primacy.[23]

Whatever explains the centrality of confidentiality in breach response, this focus has major downsides. Relying on over sixty interviews with a broad range of actors in the cybersecurity landscape — including lawyers, forensic investigators, insurers, and regulators — this Article shows how, in their efforts to preserve the confidentiality of their clients' incident-response efforts, lawyers may undermine the long-term cybersecurity of their clients and society more broadly.[24]

---

21. *See* NETDILIGENCE, NETDILIGENCE CYBER CLAIMS STUDY 2022 REPORT 18–21, https://netdiligence.com/wp-content/uploads/2022/10/NetD_2022_Claims_Study_1.0_PUBLIC.pdf [https://perma.cc/2HB5-8JWU] (showing that the costs of business disruption caused by ransomware attacks are higher than those of litigation); *see also* Daniel W. Woods, Tyler Moore & Andrew C. Simpson, *The County Fair Cyber Loss Distribution: Drawing Inferences from Insurance Prices*, 2 DIGIT. THREATS: RSCH. & PRAC., June 2021, at 10:7 (2021) https://dl.acm.org/doi/pdf/10.1145/3434403 [https://perma.cc/V6JQ-AHM6] (showing that litigation coverage costs more than other types of coverage for ransomware, crisis management, notification costs, and other costs); Josephine Wolff & William Lehr, *Roles for Policymakers in Emerging Cyber Insurance Industry Partnerships*, 46TH RSCH. CONF. ON COMMC'N, INFO. & INTERNET POL'Y 1, 21–22 (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3141409 [https://perma.cc/9XN3-KQXQ] (showing that insurers prioritize partnerships with law firms to reduce costs caused by legal risks associated with data breaches).

22. *See* Paul Vaaler & Brad Greenwood, Do US State Breach Notification Laws Decrease Firm Data Breaches? (Mar. 6, 2023) (unpublished manuscript) (on file at SSRN), https://www.ssrn.com/abstract=3885993 [https://perma.cc/EZ26-KHAT].

23. *See infra* Part III (discussing this possibility).

24. While we are the first to empirically study this reality, we are not the first to hypothesize that legal rules governing confidentiality could undermine cybersecurity. For instance, in a 2016 article, Jeff Kosseff argued that "current evidentiary law discourages companies from investing in the services necessary to prevent cyberattacks from occurring." Jeff Kosseff, *The Cybersecurity Privilege*, 12 J.L. & POL'Y. INFO. SOC'Y 261, 261–62 (2016). A 2020 report from the Sedona Conference Working Group on Data Security and Privacy Liability also noted that the legal uncertainty surrounding privilege and work-product immunity could have a substantial impact on how breach investigations are conducted. *See* The Sedona Conference, *Commentary on Application of Attorney-Client Privilege and Work-Product Protection to Documents and Communications Generated in the Cybersecurity Context*, 21 SEDONA CONF. J. 1, 82–86 (2020) [hereinafter *Sedona Report*]. And several articles directed to legal experts had even encouraged attorneys to skip commissioning a forensic report altogether to protect the company's confidential information. *See* Ben Kochman, *It's Getting Harder To Hide Consultants' Data Breach Reports*, LAW360 (June 3, 2020, 10:10 PM), https://www.law360.com/articles/1279264 [https://perma.cc/WFA6-3JTW]. Some courts, however, have dismissed these concerns. *See In re* Cap. One Consumer Data Sec. Breach Litig., No. 19md2915, 2020 WL 3470261, at *7 n.8 (E.D. Va. June 25, 2020).

This outcome largely stems from lawyers' efforts to orchestrate a cyber-incident response to maximize the chances that attorney-client privilege and work-product protections will attach. Toward this end, we find that lawyers frequently direct forensic providers to refrain from making recommendations to clients about how to enhance their cyber defenses, restrict direct communications between forensic firms and clients, insist upon hiring forensic firms with limited familiarity with the client's networks or internal processes, and strictly limit dissemination of the forensic firm's conclusions to the client's internal personnel. To ensure that clients do not inadvertently waive any legal confidentiality protections, lawyers also routinely refuse to share any written documentation regarding a breach with third parties like insurers, regulators, and law enforcement.[25] Collectively, these lawyer-driven strategies impair impacted firms' abilities to learn from cybersecurity incidents and implement long-term remediation efforts. Furthermore, they inhibit insurers' efforts to understand the efficacy of different security countermeasures[26] and regulators' capacity to investigate cybersecurity incidents.[27]

Unfortunately for lawyers (and their clients), these breach response strategies do not, in fact, always succeed in triggering attorney-client privilege or work-product protections.[28] At bottom, this is because cyber-incident response virtually always involves a thorny blend of legal and business considerations, which fundamentally rely on the technical expertise only third-party cybersecurity firms can supply. Yet the rules governing attorney-client privilege and work-product doctrine require courts to assess whether the driving purpose of communications produced during a cyber-incident response involve the provision of legal services or preparation for litigation, as opposed to business-oriented goals.[29] Answering this question is often immensely difficult

25. On the importance of information sharing to cybersecurity, see Elaine M. Sedenberg & Deirdre K. Mulligan, *Public Health as a Model for Cybersecurity Information Sharing*, 30 BERKELEY TECH. L.J. 1687, 1691 (2015).

26. On the potential and actual role of cyberinsurers in managing cyber risk, see Kenneth Abraham & Daniel Schwarcz, *The Limits of Regulation by Insurance*, 98 IND. L.J. 215, 231–33 (2022); Asaf Lubin, *Insuring Evolving Technology*, 28 CONN. INS. L.J. 130, 162–63 (2022); Shauhin Talesh & Bryan Cunningham, *The Technologization of Insurance: An Empirical Analysis of Big Data and Artificial Intelligence's Impact on Cybersecurity and Privacy*, 5 UTAH L. REV. 967, 975 (2021); Shauhin A. Talesh, *Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Business*, 43 LAW & SOC. INQUIRY 417, 425–35 (2018); Jay P. Kesan & Carol M. Hayes, *Strengthening Cybersecurity with Cyberinsurance Markets and Better Risk Assessment*, 102 MINN. L. REV. 191, 273–76 (2017).

27. Of course, there is a natural limit to the effectiveness of efforts to limit future breaches, given that many are caused by human error. *See* Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011, 1019–20 (2014); Paul Ohm, *The Myth of the Superuser: Fear, Risk, and Harm Online*, 41 U.C. DAVIS L. REV. 1327, 1331–32 (2008).

28. *See Sedona Report*, *supra* note 24, at 30.

29. *See infra* Part II.

because most breach investigations implicate an interconnected web of legal and nonlegal goals.

The uncertain protections that attorney-client privilege and work-product immunity provide for lawyer-coordinated breach response efforts is nicely illustrated by the pivotal 2020 case, *In re Capital One*.[30] That case arose from a 2019 breach of Capital One's computer systems, which resulted in the theft of personal data belonging to 100 million of its customers, including credit card applications, social security numbers, and bank account numbers.[31] The day after it discovered this breach, Capital One retained the prominent law firm Debevoise & Plimpton, which attempted to shield Capital One's breach response efforts from discovery in a subsequent lawsuit.[32] Toward that end, Debevoise and Capital One together retained the leading cybersecurity firm Mandiant under a tripartite agreement that instructed Mandiant to investigate the breach at Debevoise's direction.[33] After months of investigation, Mandiant wrote a final report that included a thorough timeline of the breach as well as an analysis of where Capital One's lines of defense and security controls failed, the extent of the compromise, and remediation steps that the company should take moving forward.[34] That report went first to Debevoise, which subsequently shared it with a select group within Capital One, including its legal department, board of directors, and certain technical employees.[35]

Despite Debevoise following standard practices for engaging the forensic firm and controlling the dissemination of the Mandiant incident report, its efforts to shield the report from discovery were unsuccessful. In a subsequent class action lawsuit, the United States District Court for the Eastern District of Virginia ordered Capital One to turn over the report to plaintiffs.[36] The court reasoned that the Mandiant

---

30. *See In re* Cap. One Consumer Data Sec. Breach Litig., No. 19md2915, 2020 WL 3470261, at *3–6 (E.D. Va. June 25, 2020). *In re Capital One* was not the first case to conclude that cybersecurity breach reports commissioned by an impacted firm's lawyers could not be shielded from discovery in subsequent litigation. *See, e.g.*, *In re* Premera Blue Cross Customer Data Sec. Breach Litig., 296 F. Supp. 3d 1230, 1249 (D. Or. 2017); *In re* Dominion Dental Servs. USA, Inc. Data Breach Litig., 429 F. Supp. 3d 190, 194–96 (E.D. Va. 2019).

31. Emily Flitter & Karen Weise, *Capital One Data Breach Compromises Data of Over 100 Million*, N.Y. TIMES (July 29, 2019), https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html [https://perma.cc/2FYM-ZBJ6].

32. *In re Cap. One*, 2020 WL 3470261, at *1.

33. *Id.* at *1–2.

34. Some of Mandiant's incident reports are publicly available, such as one the firm authored in 2012 about a breach of the South Carolina Department of Revenue's computer systems and another it published in 2013 about Chinese cyberespionage. *See, e.g.*, MARSHALL HEILMAN & CHRISTOPHER GLYER, MANDIANT, SOUTH CAROLINA DEPARTMENT OF REVENUE: PUBLIC INCIDENT RESPONSE REPORT (2012), https://oag.ca.gov/system/files/Mandiant%20Report_0.pdf [https://perma.cc/39TL-B5RP]; MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS (2013), https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf [https://perma.cc/VX6U-UBFM].

35. *See In re Cap. One*, 2020 WL 3470261, at *2.

36. *See id.* at *1.

report could not be withheld from plaintiffs because its "driving force" involved business, rather than legal, considerations, as Capital One had failed to show that the report would not have been "created in essentially the same form in the absence of litigation."[37] In reaching this conclusion, the court emphasized that the report was disseminated to various Capital One technical and management employees and that Capital One had a retainer agreement with Mandiant in place before it was breached.[38]

The *In re Capital One* case, we find, marked a significant turning point in how confidently lawyers and breached organizations viewed the confidentiality protections that they could provide for incident-response investigations they spearheaded.[39] This uncertainty has had two related effects. First, it convinced many lawyers to adopt even more aggressive strategies than Debevoise did to maximize the chances of triggering attorney-client privilege or work-product protections.[40] These include more strictly limiting the internal personnel to whom breach-related materials are disseminated, hiring forensic firms that have no prior relationship with the breached firm, and explicitly communicating that the forensic firm's sole role is to assist counsel in providing legal services to the client.

Second, and even more troublingly, *In re Capital One* accelerated lawyers' attempts to protect the confidentiality of their clients' breach response efforts in ways that do not rely on legal doctrines. Of particular note, we find that lawyers overseeing breach investigations often tell forensic firms not to craft a final report or issue written recommendations to the client, especially when the findings suggest that the client had a particularly poor security posture to begin with.[41] To be sure, lawyers conducting internal investigations often opt for oral rather than written reports to limit disclosure risk in litigation.[42] But lawyers who impose this practice on forensic firms' breach response efforts, we

37. *Id.* at *3 (citing RLI Ins. Co. v. Conseco, Inc., 477 F. Supp. 2d 741, 747–48 (E.D. Va. 2007)).

38. *See id.* at *6.

39. *See* Kochman, *supra* note 24. Even prior to *In re Capital One*, scholars and practitioners had emphasized the indeterminacy of whether pre- and post-breach cybersecurity efforts could be shielded from discovery. For instance, in a 2016 article, Kosseff identified gaps in the existing attorney-client privilege and work-product protections for cybersecurity-related work. *See* Kosseff, *supra* note 24, at 261. Similarly, a detailed 2020 report from the Sedona Conference Working Group on Data Security and Privacy Liability noted that "certainly there is no 'settled law' in the cybersecurity area that establishes, when, if ever, a breached organization's pre- and post-breach cybersecurity-related documents and communications . . . can be protected from discovery under the attorney-client privilege or the work-product protection." *Sedona Report*, *supra* note 24, at 11.

40. *See infra* Part III.

41. *See infra* Part III.

42. *See* O'MELVENY & MYERS LLP, IN-HOUSE COUNSEL'S GUIDE TO CONDUCTING INTERNAL INVESTIGATIONS 49 (2020) (suggesting that litigation risk leads to "the convention . . . of provid[ing] an oral report where possible").

conclude, dramatically impair the ability of both breached firms and third parties to prevent future cyberattacks.

We detail these conclusions in three Parts. Part II lays the foundation for the analysis by examining attorney-client privilege and work-product doctrines in the context of pre- and post-breach cybersecurity efforts. In doing so, Part II emphasizes the uncertainty that this law creates concerning firms' abilities to shield their incident-response efforts from litigants or other actors, and the potential impact of selectively sharing such materials with trusted third parties like insurers or law enforcement. This uncertainty, Part II notes, is absent from the pre-breach setting, where the law is relatively clear that most pre-breach cybersecurity efforts cannot be shielded from discovery.

The heart of the Article is contained in Part III, which details our empirical strategy and results. Relying on over sixty interviews with a broad range of actors in the cybersecurity landscape, it explores the impact of the legal uncertainty illustrated in *In re Capital One* and lawyers' resulting efforts to preserve the confidentiality of firms' post-breach cybersecurity efforts. These strategies, Part III shows, substantially impact everyone involved in incident response, including the forensic specialists carrying out those investigations, the impacted firms' personnel who are tasked with remediating the breach and bolstering firms' cybersecurity, the insurers responsible for covering costs associated with these incidents, and regulators who may want to further investigate the breaches. Part III also details how these effects can, and often do, weaken the cybersecurity efforts of both impacted firms and society more broadly. By contrast, Part III finds limited evidence that confidentiality concerns significantly impact firms' pre-breach cybersecurity efforts.

Finally, Part IV considers possible interventions to address the challenges that confidentiality concerns create for cybersecurity. We ultimately suggest that the materials produced during incident response should be entitled to confidentiality protections that are untethered from the provision of legal services, but that such protections should be coupled with new requirements that breached firms disclose specific forensic evidence and analysis. By disentangling the incident-response process from the production of information that can hold firms accountable for failing to take appropriate and required precautions, this Article aims to remove existing barriers to effective incident response while preserving incentives for firms to take cybersecurity seriously.

II. UNCERTAIN DOCTRINE: THE LAW GOVERNING THE CONFIDENTIALITY OF FIRMS' CYBERSECURITY EFFORTS

Firms have innumerable reasons for wanting to keep their cybersecurity efforts confidential: doing so helps to limit the risk of litigation,

negative publicity, and regulatory actions.[43] The two primary legal tools that firms use to help achieve this goal are familiar to lawyers: the attorney-client privilege and work-product doctrine. The former protects all oral and written communications between privileged persons that are made in confidence to provide or obtain legal advice.[44] Crucially, this privilege extends to communications between attorneys and third-party consultants, such as cybersecurity firms, that attorneys rely upon to provide clients with legal advice.[45] Work-product immunity provides distinct, but often overlapping, assurances of confidentiality. It shields from discovery documents or mental processes of attorneys and their consultants that are prepared in reasonable anticipation of litigation or for trial.[46] Like the attorney-client privilege, work-product immunity can preserve the confidentiality of cybersecurity professionals' efforts to the extent that those efforts can be tied to actual or anticipated litigation.

Because confidentiality concerns figure so prominently in cybersecurity generally, and in cyber-incident response in particular, a significant body of caselaw has developed in recent years that elaborates on the applicability of attorney-client privilege and work-product immunity in these settings. Nonetheless, central questions regarding the protections afforded by these doctrines in the cybersecurity setting remain unclear.[47] This is partly because the rules governing these doctrines vary across states and between federal and state courts.[48] Courts applying these doctrines frequently embrace vague multi-factored tests, resulting in courts reaching seemingly inconsistent holdings in apparently similar cases while latching onto factual distinctions that even the most sophisticated firms and lawyers fail to anticipate.[49] Finally, some key legal questions — such as the applicability of the common interest doctrine to communications between breach counsel and cyberinsurers — remain largely unanswered in the caselaw due to commonly accepted, though highly contestable, narratives about what practices are necessary to preserve confidentiality.[50]

This Part elaborates on these assessments of the caselaw. Section A starts by reviewing when involving an attorney in the hiring or direction of a cybersecurity consultant's work in the aftermath of a potential

---

43. *See, e.g.*, Melanie L. Cyganowski, Erik B. Weinick & Aisha Khan, *Protecting Privilege in Cyberspace, the Age of COVID-19 and Beyond*, NY LITIGATOR (Jan. 15 2021), https://nysba.org/protecting-privilege-in-cyberspace-the-age-of-covid-19-and-beyond [https://perma.cc/PQ7F-3MFB]; Brian Mund & Leonard Bailey, *Privilege in Data Breach Investigations*, 69 DEP'T JUST. J. FED. L. & PRAC. 39, 39–40 (2021).

44. RESTATEMENT (THIRD) OF THE L. GOVERNING LAWS. § 68 (AM. L. INST. 2000).

45. *See, e.g.*, United States v. Kovel, 296 F.2d 918, 922 (2d Cir. 1961).

46. FED. R. CIV. P. 26(b)(3).

47. *See Sedona Report*, *supra* note 24, at 8.

48. *See* Timothy P. Glynn, *Federalizing Privilege*, 52 AM. U. L. REV. 59, 60 (2002).

49. *See infra* Section II.A.

50. *See infra* Section II.C.

breach will result in that work being privileged or protected by attorney-client privilege or work-product immunity. Section B then considers when a cybersecurity consultant's work before a potential breach may be deemed confidential. Finally, Section C considers the law, or lack thereof, regarding when and whether disclosures of a cybersecurity consultant's work product to third parties can jeopardize any confidentiality protections that would otherwise apply.

A. Attorney-Client Privilege and Work-Product Immunity for Incident Response

When businesses suspect that they have experienced a cyber incident, their first call is often to a lawyer.[51] These lawyers then coordinate all elements of the impacted firm's cyber-incident response, including retaining and directing the efforts of a third-party cybersecurity firm.[52] As described above, a principal goal of using lawyers to coordinate breach response is to ensure that information that is produced during this process is shielded from discovery by either attorney-client privilege or work-product immunity.[53]

In reality, however, it is often unclear when or whether advice received from cybersecurity experts in the aftermath of a breach will be protected by either attorney-client privilege or work-product immunity.[54] Fundamentally, this is because breach investigations inevitably implicate an interconnected web of legal and nonlegal goals. Yet only investigations designed to facilitate the provision of legal advice (in the case of the attorney-client privilege) or to prepare for actual or reasonably anticipated litigation (in the case of the work-product doctrine) are entitled to legal assurances of confidentiality.[55] Courts facing assertions of attorney-client privilege or work-product immunity concerning materials produced in post-breach investigations must consequently balance the primacy of the legal and nonlegal goals that drove a particular

---

51. *See* Daniel W. Woods & Rainer Böhme, *Incident Response as a Lawyers' Service*, 20 IEEE SEC. & PRIV. 68, 68 (2022); Daniel W. Woods & Rainer Böhme, *How Cyber Insurance Shapes Incident Response: A Mixed Methods Study*, *in* 20TH WORKSHOP ON ECON. INFO. SEC. 10–12 (2021).

52. *See* sources cited *supra* note 43.

53. *See* sources cited *supra* note 43.

54. Even when these protections attach, they are subject to various potential limitations and exceptions. For instance, attorney-client privilege does not extend to facts within privileged communications. *See Sedona Report*, *supra* note 24, at 14. And work-product immunity can be surmounted by plaintiffs who can show they have a substantial need for the covered information and cannot obtain the substantial equivalent through other means without undue hardship. *See* FED. R. CIV. P. 26(b)(3)(A)(i)–(ii). However, many of the underlying forensic artifacts in a breach, including "event logs and network diagrams" are available to plaintiffs, meaning that plaintiffs will rarely have a substantial need for analyses or reports of these materials. *See In re* Cap. One Consumer Data Sec. Breach Litig., No. 19md2915, 2020 WL 2731238, at *3 n.2 (E.D. Va. May 26, 2020).

55. *See* FED. R. CIV. P. 26(b)(3)(A).

investigation.[56] And they do so by considering a broad range of factors that vary across jurisdictions and courts.[57] Subsection One reviews these factors. Subsection Two then discusses how courts balance these factors when they point in opposite directions.

1. Factors for Disentangling Legal and Business Purposes of Incident Response

Courts attempting to determine whether the underlying purpose of post-breach forensic investigations qualifies them for protection under work-product immunity or attorney-client privilege have considered a broad range of fact-based, indeterminate factors. These include: (a) whether the breached firm or their external counsel hired the cybersecurity firm, and when they did so; (b) whether the breached firm or their external counsel supervised the cybersecurity firm; (c) the services that the cybersecurity firm provided; (d) the source of funding used to pay the cybersecurity firm; (e) the extent to which parties outside the cybersecurity firm worked on the investigation; (f) the content of the cybersecurity firm's reports; (g) the identity of the individuals to whom any reports or communications from the cybersecurity firm were disclosed; and (h) whether the breached business made public announcements regarding the cybersecurity firm's investigation.

a. Did External Counsel Hire the Cybersecurity Firm?

Courts often place significant weight on which party retained the cybersecurity firm and when they did so in assessing the purpose of that firm's post-breach services. Courts are more likely to consider a cybersecurity firm's post-breach services to be linked to the provision of legal services (in the case of attorney-client privilege) or to have anticipated litigation (in the case of work-product immunity) when it is hired by the breached firm's external counsel after a potential breach.[58] This can and does take the form of a tripartite agreement entered into by the breached firm, its external counsel, and the forensic firm.[59] By

56. *See* Gregory C. Sisk & Pamela J. Abbate, *The Dynamic Attorney-Client Privilege*, 23 GEO. J. LEGAL ETHICS 201, 203 (2010).

57. *See* Glynn, *supra* note 48, at 60; *see also* Michele DeStefano Beardslee, *The Corporate Attorney-Client Privilege: Third-Rate Doctrine for Third-Party Consultants*, 62 SMU L. REV. 727, 730 (2009) (footnote omitted) (noting that, in general, "it is unclear which communications between lawyers, clients, and third-party professional, strategic consultants, if any, will be protected by the attorney–client privilege or some other privilege doctrine").

58. *See, e.g.*, New Albertson's, Inc. v. MasterCard Int'l, No. 01-17-04410, slip op. at 6 (Idaho 4th Dist. Ct., Ada Cnty. May 31, 2019).

59. *See* Matthew D. Krueger, Eileen R. Ridley, Aaron K. Tantleff, Jennifer L. Urban, Steven M. Millendorf & Avi B. Ginsberg, *Maintaining Privilege Over Forensic Reports*, BLOOMBERG L. (Sept. 2021), https://www.foley.com/en/insights/publications/2021/09/maintaining-privilege-over-forensic-reports [https://perma.cc/N9RX-2EXQ].

contrast, courts are often highly skeptical of claims that a cybersecurity firm's work was driven by legal purposes when it was hired directly by a firm before it experienced a breach, and was only asked after a potential breach to assist that firm's external counsel.[60]

Applying these principles becomes difficult in cases where a cybersecurity vendor provides pre-breach services to a firm but is subsequently asked to provide post-breach services pursuant to a new tripartite agreement involving outside counsel. Some courts regard such maneuvers as legitimately indicating that the purpose of a forensic firm's services has shifted from providing business services to facilitating the provision of legal services.[61] Other courts, however, interpret these circumstances to suggest that the forensic firm was, in practice, hired by the breached firm to provide nonlegal services.[62] These courts have suggested that firms should hire different cybersecurity firms for pre-breach surveillance versus post-breach communications if they wish to ensure that the latter is shielded from discovery.[63]

b. Did External Counsel Supervise the Cybersecurity Firm?

In addition to considering whether external counsel hired a cybersecurity firm after a breach, courts also assess the purpose of a cybersecurity firm's work under the attorney-client privilege and work-product doctrine by evaluating whether external counsel *managed* its work. To do so, courts often look first to the terms of the cybersecurity firm's contract. Courts are more likely to shield a cybersecurity firm's work from discovery when contractual terms specify that its work will be done solely at the direction of external counsel.[64]

However, courts typically also look beyond the formal governing agreement to assess whether external counsel in fact managed all elements of a cybersecurity firm's work.[65] Courts are particularly wary of

60. *See, e.g.*, *In re* Cap. One Consumer Data Sec. Breach Litig., No. 19md2915, 2020 WL 3470261, at *7 (E.D. Va. June 25, 2020).

61. *See, e.g.*, *New Albertson's*, slip op. at 6–7 (finding that a forensic firm's communications were privileged when it had previously provided pre-breach services but was rehired by external counsel after a potential breach); *In re* Experian Data Breach Litig., No. 15-01592, 2017 WL 4325583, at *3 (C.D. Cal. 2017) ("Mandiant's previous work for Experian was separate from the work it did for Experian regarding this particular data breach.").

62. *See, e.g.*, *In re Cap. One*, 2020 WL 3470261, at *1; Wengui v. Clark Hill, PLC, 338 F.R.D. 7, 13–14 (D.D.C. 2021).

63. The *In re Capital One* court encouraged businesses like Capital One to "produce and protect work product . . . through *different* vendors, *different* scopes of work and/or *different* investigation teams." *In re Cap. One*, 2020 WL 3470261, at *6 n.8 (emphasis added).

64. *See In re* Premera Blue Cross Customer Data Sec. Breach Litig., 296 F. Supp. 3d 1230, 1245–46 (D. Or. 2017) (suggesting that a Statement of Work ("SOW") listing external counsel as the forensic firm's supervisor was relevant to the privilege analysis).

65. *In re* Cap. One Consumer Data Sec. Breach Litig., No. 19md2915, 2020 WL 2731238, at *4 (E.D. Va. May 26, 2020) ("[The] only significant evidence that Capital One has

parties naming counsel as a cybersecurity firm's supervisor to immunize communications from discovery, when the realities of the parties' arrangement suggest that the breached firm is actually directing the cybersecurity firm's work.[66] For that reason, counsel must not only be listed in the governing agreement as the cyber firm's exclusive supervisor, but the evidence must suggest that this writing reflected reality.[67]

c. Nature of Cybersecurity Firms' Services

Not surprisingly, one of the most significant factors that courts consider in evaluating the purpose of a cybersecurity firm's work is the scope of that work. Courts often focus this inquiry on the written description of services the cybersecurity firm has agreed to provide in its contract.[68] In doing so, courts evaluate whether these services are associated with supporting fundamentally business functions on the one hand or facilitating external counsel's provision of legal services (in the case of attorney-client privilege) or preparation for litigation (in the case of work-product immunity), on the other hand.[69] Unprivileged business-related services include discovering how the breach occurred, remediating the consequences of breach, formulating public statements, and making recommendations to ensure a breach cannot happen again.[70] By contrast, privileged legal or litigation services include helping lawyers to respond to regulatory authorities, preparing for anticipated litigation, or understanding the scope of the breached firms' duties under state breach notification laws.[71] Meanwhile, some services, such as notifying customers regarding the scope of a breach, may frequently blend legal and nonlegal services.

In cases where a cybersecurity firm has previously provided business services to the breached company, courts also evaluate whether the formal description of services adopted in the aftermath of a breach

---

presented concerning the work Mandiant performed is that the work was at the direction of outside counsel . . . .").

66. *See, e.g.*, *In re* Dominion Dental Servs. USA, Inc. Data Breach Litig., 429 F. Supp. 3d 190, 194 (E.D. Va. 2019) ("The addition of language referencing 'under the direction of Counsel' appears to be designed to help shield material from disclosure rather than to fundamentally alter the business purposes of the work."); *Wengui*, 338 F.R.D. at 13 ("Although [the breached business] papered the arrangement [with the security firm] using its attorneys, that approach 'appears to [have been] designed to help shield material from disclosure' . . . ." (quoting *In re Dominion*, 429 F. Supp. 3d at 194)).

67. *See, e.g.*, *In re Dominion*, 429 F. Supp. 3d at 195; *Wengui*, 338 F.R.D. at 13. *See generally* Upjohn Co. v. United States, 449 U.S. 383, 395 (1981) (warning corporations that facts are not automatically protected from disclosure when counsel directs an investigation).

68. *See, e.g.*, *In re* Marriott Int'l, Inc. Customer Data Sec. Breach Litig., No. 19-MD-2879, 2021 WL 2660180, at *5 (D. Md. June 29, 2021); *In re Cap. One*, 2020 WL 3470261, at *6.

69. *Sedona Report*, *supra* note 24, at 58–69.

70. *See, e.g.*, *In re* Premera Blue Cross Customer Data Sec. Breach Litig., 296 F. Supp. 3d 1230, 1242–43 (D. Or. 2017); *Wengui*, 338 F.R.D. at 11–12.

71. *See In re Marriott*, 2021 WL 2660180, at *6.

fundamentally altered the security firm's responsibilities.[72] If not, courts often conclude that the cybersecurity firm's work remains business related, and hence discoverable.[73] Slight alterations in the contract language indicating, for instance, that the cybersecurity firm's services will be conducted "at the direction of counsel," may not be sufficient to convince courts that legal- or litigation-oriented purposes really drive the work.[74]

Courts vary in the extent to which they look beyond formal contract language to assess whether that language accurately reflects the work that a cybersecurity firm has provided. In some cases, courts have rejected work-product immunity claims when the formal description of services failed to sufficiently acknowledge litigation risk, despite evidence that this risk played a significant role in retaining the firm.[75] At the same time, courts are sometimes unwilling to defer to the formal description of services to be performed by a cybersecurity firm when there is evidence that this description is inaccurate.[76] And in many cases, courts take seriously arguments that a contract purporting to hire a cybersecurity firm to provide legal or litigation services, rather than business services, is a "sham," even if they do not always find such arguments convincing.[77]

---

72. *See, e.g.*, *In re Cap. One*, 2020 WL 3470261, at *1, *6.

73. *See, e.g.*, *In re* Dominion Dental Servs. USA, Inc. Data Breach Litig., 429 F. Supp. 3d 190, 194 (E.D. Va. 2019) (declining to apply work-product immunity when the formal descriptions of services for a cybersecurity firm before and after the data breach were "almost identical," with the main difference being "the inclusion of small modifying phrases such as 'if requested by Counsel'"); *In re* Cap. One Consumer Data Sec. Breach Litig., No. 19md2915, 2020 WL 2731238, at *1, *6–7 (E.D. Va. May 26, 2020) (rejecting work-product claim where Capital One initially hired Mandiant in 2015 to provide "incident response services" but subsequently entered into a tripartite Letter Agreement involving its counsel in the aftermath of a breach, in part because Mandiant agreed to provide "virtually identical" services before and after the breach that involved "computer security incident response; digital forensics, log, and malware analysis support; and incident remediation assistance").

74. *See, e.g.*, *In re Dominion*, 429 F. Supp. 3d at 195.

75. *See In re* Rutter's Data Sec. Breach Litig., No. 20-CV-382, 2021 WL 3733137, at *2 (M.D. Pa. July 22, 2021) (rejecting work-product immunity in part because the description of services in the governing agreement indicated that counsel did not know whether its client's defenses had been breached when it hired cybersecurity firm and thus whether it was under the threat of litigation, despite testimony implying the parties knew a breach occurred).

76. *Compare* Genesco, Inc. v. Visa U.S.A., Inc., 302 F.R.D. 168, 181 (M.D. Tenn. 2014) (emphasizing express statement in the retainer agreement that the investigation was "in anticipation of potential litigation and/or legal or regulatory proceedings"), *with In re Cap. One*, 2020 WL 3470261, at *5 (dismissing the relevance of a provision in the SOW providing that "the work was at the direction of outside counsel").

77. *In re* Marriott Int'l, Inc. Customer Data Sec. Breach Litig., No. 19-MD-2879, 2021 WL 2660180, at *3 (D. Md. June 29, 2021) (rejecting claim that Marriott's "attorneys engage in sham agreements with vendors on its behalf to perform work that was already to occur under pre-existing obligations" and that involved fundamentally business purposes).

d. Who Paid for the Cybersecurity Firm?

A fourth factor that may play a role in judicial assessments of work-product and privilege claims involving post-breach forensic investigations is which party paid for the cybersecurity firm's services and how those payments were internally recorded. Recent cases have implied that a breached firm's direct payment to a forensic investigator may indicate that business rather than legal considerations drove its services.[78] Similarly, the *In re Capital One* court highlighted that Capital One initially paid its cybersecurity firm out of its "business critical" expense and cyber organization budget, but subsequently paid it from its legal department budget after it was breached.[79] By contrast, some cases have indicated that a law firm's direct payment of a cybersecurity firm may indicate that the cybersecurity firm was indeed hired solely to facilitate the provision of legal advice or prepare for anticipated litigation.[80] In some cases, breach attorneys indicated they would directly pay the cybersecurity firm on behalf of their client to make clear that the forensic investigators had been retained solely to provide legal advice.[81]

e. Did the Cybersecurity Firm Work with Persons Other than External Counsel?

Yet another factor that courts sometimes consider in evaluating the legal or business purpose of a cybersecurity firm's post-breach investigations is the extent of its contacts with individuals other than external counsel. When a cybersecurity firm works with individuals other than external counsel or the breached business, courts have interpreted this to mean that its investigation was not principally intended to assist external counsel in preparing for potential litigation.[82] Other cases suggest that a cybersecurity firm that works closely with the breached firm's information technology personnel in the aftermath of a breach is

78. *See In re Rutter's*, 2021 WL 3733137, at *1 (noting that "[d]efendant paid [the firm] directly" but not clarifying the relevance of this fact, if any, to the analysis).

79. *In re Cap. One*, 2020 WL 3470261, at *1.

80. *Cf.* United States v. Kovel, 296 F.2d 918, 922 (2d Cir. 1961) ("[T]he presence of an accountant, whether hired by the lawyer or by the client, while the client is relating a complicated tax story to the lawyer, ought not destroy the privilege . . . .").

81. For instance, one attorney said that after the *In re Capital One* decision "sometimes the payment to the forensic team comes directly from the company but sometimes now we will pay the forensic team (after the client pays us for the forensic team fees)." Zoom Interview with Breach Att'y 14 (Jan. 6, 2022).

82. *See, e.g.*, Wengui v. Clark Hill, PLC, 338 F.R.D. 7, 13–14 (D.D.C. 2021).

more likely to be deemed to be providing business rather than legal or litigation preparation services.[83]

f. Content of Cybersecurity Reports or Writings

Courts frequently consider the substance of a cybersecurity firm's written reports when evaluating claims of privilege and work-product immunity. Courts are less likely to shield these reports from discovery when they are technical and focus predominantly on establishing facts related to a breach.[84] With respect to attorney-client privilege, this trend reflects the broader principle that facts cannot be privileged.[85] As for work-product immunity, the fact-based nature of a report may indicate that the cybersecurity firm would have been retained to provide the same services even in the absence of potential litigation.[86]

Courts are also reluctant to shield reports from discovery that include significant recommendations for remediating network security vulnerabilities. Such recommendations suggest to some courts that the breached business's "true objective was gleaning [the firm's] expertise in cybersecurity, not in 'obtaining legal advice.'"[87] Other courts, however, do treat reports containing recommendations as privileged, though they are not often transparent about their reasoning for doing so.[88]

g. Disclosure of Materials Produced by Cybersecurity Firms

In addition to the substance of a forensic report, courts also consider the extent of the report's dissemination when making privilege and immunity determinations. The greater the number of individuals with access to a forensic report, the greater the likelihood courts will

---

83. *See, e.g.*, *In re Rutter's*, 2021 WL 3733137, at *1–4 (rejecting attorney-client privilege and work-product immunity protections where the security firm worked "alongside Rutter's IT personnel" and met directly with the breached business "numerous" times).

84. *See, e.g.*, *In re* Dominion Dental Servs. USA, Inc. Data Breach Litig., 429 F. Supp. 3d 190, 192 n.4 (E.D. Va. 2019) ("[T]he contents of the report itself reflects [sic] that the information is entirely factual [and] relates directly to the business interests of the defendants . . . .").

85. *See* Upjohn Co. v. United States, 449 U.S. 383, 395 (1981).

86. *In re* Cap. One Consumer Data Sec. Breach Litig., No. 19md2915, 2020 WL 2731238, at *4 (E.D. Va. May 26, 2020) (suggesting that Mandiant's report would have been created in a substantially similar form in the absence of litigation because it detailed "the technical factors that allowed the criminal hacker to penetrate Capital One's security" (quoting Cantwell Decl.¶ 19, *In re Cap. One*, 2020 WL 2731238 (No. 19md2915))).

87. *Wengui*, 338 F.R.D. at 13–14 (quoting Linde Thomson Langworthy Kohn & Van Dyke, P.C. v. Resol. Tr. Corp., 5 F.3d 1508, 1514–15 (D.C. Cir. 1993)).

88. *See, e.g.*, *In re* Marriott Int'l, Inc. Customer Data Sec. Breach Litig., No. 19-MD-2879, 2021 WL 2660180, at *6 (D. Md. June 29, 2021) (acknowledging that the report included recommendations for the business's security systems, but nonetheless treating the report as privileged).

find the report serves a business, rather than a legal, purpose.[89] This logic played a key role in the *In re Capital One* decision. Dissemination of Mandiant's report to Capital One's in-house counsel, board of directors, and dozens of technical employees, the court held, was "appropriately probative of the purposes for which the work product was initially produced."[90]

The method of a report's disclosure is also relevant to whether it can be shielded from discovery. Courts are more likely to treat reports as confidential if the cybersecurity firm transmits them directly to external counsel, even if external counsel then shares the report with the client.[91] By contrast, some courts have expressed skepticism regarding the legal purpose of a cybersecurity firm's services when it shares its final report directly with the breached business's personnel.[92] However, this may be less true if the report shared with the breached firm's personnel includes redacted materials relevant to legal strategy.[93]

h. External Communications Regarding Cybersecurity Firm

Another potentially relevant factor is whether a breached company publicizes the retention of a cybersecurity firm in the wake of a data breach. Broadcasting such a move may indicate to a court that its purpose is to appeal to customers rather than to facilitate the provision of legal services or prepare for the threat of litigation. That, at least, is the implication of *In re Dominion Dental*, where the court latched on to the company's communications with its clients, which included statements that the firm had hired a "world leading cybersecurity firm" and would continue to share "information regarding the status of the investigation" to customers.[94] Most courts have not, however, explicitly noted this factor in their analysis, suggesting that its influence may be minimal.

---

89. *See Wengui*, 338 F.R.D. at 12 (rejecting work-product immunity for the firm's report that was shared with the breached business's IT staff and the FBI).

90. *In re* Cap. One Consumer Data Sec. Breach Litig., No. 19md2915, 2020 WL 3470261, at *6 (E.D. Va. June 25, 2020).

91. *See, e.g.*, *In re* Experian Data. Breach Litig., No. SACV 15-01592, 2017 WL 4325583, at *3 (C.D. Cal. May 18, 2017).

92. *In re* Rutter's Data Sec. Breach Litig., No. 20-CV-382, 2021 WL 3733137, at *3 (M.D. Pa. July 22, 2021) (concluding that cybersecurity firm's direct disclosure of report to Rutter's demonstrated that the report lacked a primary legal purpose).

93. *In re Experian*, 2017 WL 4325583, at *2 (granting work-product immunity when a redacted version of the report was provided to the business's internal incident-response team).

94. *In re* Dominion Dental Servs. USA, Inc. Data Breach Litig., 429 F. Supp. 3d 190, 192–95 (E.D. Va. 2019) ("Defendants' case is further undermined by" the fact that they "publicized the retention and work of Mandiant for 'non-litigation purpose[s]' such as reassuring customers and communications strategy."). The court in *In re Capital One* notes the company similarly created "talking points" based on an internal report regarding the data breach conducted by Capital One's Cyber Organization team. *See In re Cap. One*, 2020 WL 3470261, at *5 n.5. However, the *In re Capital One* court did not give weight to the creation of talking points for a public announcement of the data breach, likely because the talking points were not based on Mandiant's report.

2. Balancing Competing Factors

In addition to evaluating the multitude of factors regarding whether a cybersecurity firm's post-breach services were driven by legal or business purposes, courts confronting claims of attorney-client privilege or work-product immunity must determine how to balance these factors when they point in competing directions. Here too, the analysis is often opaque, with courts articulating varying standards for how strongly a legal, rather than a business, purpose must predominate before confidentiality protections attach. Moreover, this analysis often differs with respect to attorney-client privilege, on the one hand, and work-product immunity, on the other.

Concerning the attorney-client privilege, many courts have suggested that the relevant factors must lean almost entirely toward the provision of legal advice rather than business services for the privilege to attach. Some courts explain this point by noting that communications must be made for the "predominant purpose" of obtaining legal advice in order to be privileged.[95] Others further specify that even limited evidence that a cybersecurity firm prepared a document "for a purpose other than or in addition to obtaining legal advice" will negate privilege.[96] However, the extent to which courts broadly embrace these formulations is varied, as the scope of the privilege varies significantly across different jurisdictions.[97] Moreover, the principles governing the broader question of when communications are made for the purpose of obtaining or providing legal, rather than business, advice vary significantly across these jurisdictional domains.[98]

By contrast, most courts suggest that the balance between litigation- and business-oriented purposes underlying breach investigations need only lean moderately toward litigation for work-product immunity to attach. The rules governing work-product immunity are more uniform than those governing attorney-client privilege, as they derive from the applicable rules of civil procedure, and most states pattern their

95. *In re* County of Erie, 473 F.3d 413, 419–20 (2d Cir. 2007).

96. *In re* Premera Blue Cross Customer Data Sec. Breach Litig., 329 F.R.D. 656, 661 (D. Or. 2019) (quoting Mechling v. City of Monroe, 222 P.3d 808, 819 (Wash. Ct. App. 2009)); *cf. In re* Marriott Int'l, Inc. Customer Data Sec. Breach Litig., No. 19-MD-2879, 2021 WL 2660180, at *6 (D. Md. June 29, 2021) (finding that documents produced by IBM in response to a lawyer's request were privileged because IBM was hired to help solve a "precise, limited problem" involving how Marriott should respond to "regulatory authorities and in the litigation . . . that was anticipated").

97. Glynn, *supra* note 48, at 60. To illustrate, the Sedona Report explains that California has a more liberal approach to the attorney-client privilege when communications have a mixed legal and nonlegal purpose. *See Sedona Report*, *supra* note 24, at 17 n.16 (stating that a court must isolate "the dominant purpose *of the relationship*" to determine whether the associated communications are privileged (quoting Costco Wholesale Corp. v. Super. Ct., 219 P.3d 736, 746 (Cal. 2009))).

98. *See Sedona Report*, *supra* note 24, at 109–10.

procedures on the federal rules.[99] Nonetheless, the precise formulation that courts use to assess whether a breach investigation is conducted in response to anticipated litigation or some other goal varies slightly across different courts. For instance, in some federal circuits, this test explicitly foregoes consideration of whether "litigation was a primary or secondary motive behind the creation of a document."[100] Alternatively, courts in other federal circuits do indeed ask whether "the driving force behind the preparation of" a document was actual or anticipated litigation.[101] Either way, federal courts considering federal work-product immunity often focus the inquiry on whether, under the totality of the circumstances, "it can fairly be said that the document was created because of anticipated litigation, and would not have been created in substantially similar form but for the prospect of that litigation."[102] These courts often also require a firm's "unilateral belief"[103] that litigation that might transpire be "objectively reasonable"[104] for work-product immunity to attach.

* * * * *

In sum, the law governing when lawyers can successfully shield the breach response efforts of cybersecurity firms is complex, unpredictable, and variable. Indeed, *In re Capital One* revealed that even very sophisticated lawyers cannot always predict how a court will apply the vague and indeterminate tests associated with attorney-client privilege and work-product immunity to the complex realities of cyber-incident response.

B. Attorney-Client Privilege and Work-Product Immunity in Pre-Incident Cybersecurity Contexts

Firms occasionally involve lawyers in preventive cybersecurity efforts that take place before a potential breach occurs. For instance, firms subject to sector-specific cybersecurity regulatory regimes may hire counsel to help coordinate compliance with these rules. Alternatively,

---

99. Scott Dodson, *The Gravitational Force of Federal Law*, 164 U. PA. L. REV. 703, 711–17 (2016).

100. *In re* Experian Data. Breach Litig., No. SACV 15-01592, 2017 WL 4325583, at *1 (C.D. Cal. May 18, 2017) (quoting *In re* Grand Jury Subpoena (Mark Torf/Torf Env't Mgmt.), 357 F.3d 900, 907 (9th Cir. 2004)).

101. *In re* Cap. One Consumer Data Sec. Breach Litig., No. 19md2915, 2020 WL 3470261, at *3 (E.D. Va. May 26, 2020) (quoting Nat'l Union Fire Ins. Co. of Pittsburgh, Pa. v. Murray Sheet Metal Co., 967 F.2d 980, 984 (4th Cir. 1992)); *see, e.g.*, *In re* Rutter's Data Sec. Breach Litig., No. 20-CV-382, 2021 WL 3733137, at *2 (M.D. Pa. July 22, 2021).

102. *In re Experian*, 2017 WL 4325583, at *1 (quoting *Mark Torf*, 357 F.3d at 908).

103. *In re Rutter's*, 2021 WL 3733137, at *2 (quoting Martin v. Bally's Park Place Hotel & Casino, 983 F.2d 1252, 1260 (3d Cir. 1993)).

104. *Id.* (citing *Martin*, 983 F.2d at 1260).

firms may rely on attorneys to help negotiate contracts with significant counterparties that require them to implement certain cybersecurity precautions. Increasingly, firms also hire lawyers to proactively prepare for a potential cyber incident via tabletop exercises, penetration testing, or assessments of a firm's overall security posture.[105]

Unlike in the post-breach context, the law is relatively clear that communications regarding such pre-breach cybersecurity efforts can rarely be shielded from discovery. Work-product immunity for these services will almost never be an option, as a firm cannot reasonably anticipate litigation over its cybersecurity efforts before those efforts have failed.[106] Attorney-client privilege will also infrequently apply to the pre-breach efforts of cybersecurity professionals, even when those efforts involve lawyers.[107] Recall that communications involving third-party experts like cybersecurity firms are only privileged if they principally operate to facilitate legal advice.[108] Put simply, this is rarely the principal role of cybersecurity firms' pre-breach efforts. As the Sedona Report put it, "technical inventories, configuration reviews, vulnerability scans, and penetration tests . . . often are part of an organization's ongoing IT operations" and hence are not plausibly privileged.[109]

This conclusion likely holds even if a lawyer directs pre-breach cybersecurity efforts in connection with their client's contracts or regulatory obligations. The cybersecurity firms' communications would not be privileged because their role would not be to support the lawyer's work but to provide nonlegal services that are legally required.[110] The mere fact that nonlegal services are legally required does not mean that they are privileged, even if a lawyer coordinates their delivery.[111]

Even breach-preparation exercises, like tabletop simulations, are not principally intended to facilitate the provision of legal advice. Instead, they are intended to promote "discussions within []organizations about their ability to address a variety of threat scenarios," including "pre-incident information and intelligence sharing, incident response,

---

105. *See Sedona Report*, *supra* note 24, at 28–34 (cataloging different types of pre-breach information that lawyers may be involved in developing).

106. Work-product immunity is not available when the risk of litigation is merely speculative. *See, e.g.*, Hertzberg v. Veneman, 273 F. Supp. 2d 67, 75 (D.D.C. 2003) (explaining that the work-product doctrine requires "that litigation was 'fairly foreseeable at the time' the materials were prepared." (quoting Coastal States Gas Corp. v. Dep't of Energy, 617 F.2d 854, 865 (D.C. Cir. 1980))).

107. *See Sedona Report*, *supra* note 24, at 84. Of course, privilege will be unavailable when a cybersecurity firm's work does not involve lawyers. *Id.* at 34.

108. *See supra* Section II.A.

109. *Id.* at 35–36.

110. *See In re* Premera Blue Cross Customer Data Sec. Breach Litig., 329 F.R.D. 656, 666–67 (D. Or. 2019).

111. This analysis is in some tension with the Sedona Report, which suggests, without much explanation, that information generated "for the purpose of a legally driven or mandated security assessment, audit, or report" may be privileged. *See Sedona Report*, *supra* note 24, at 36.

and post-incident recovery."[112] Of course, there may be exceptions to these generalizations; for instance, privilege would likely attach to a security assessment produced by a cybersecurity professional solely to help the lawyer determine whether a client is complying with its legal or regulatory obligations.[113]

Consistent with this analysis, relevant cases have largely rejected attorney-client privilege or work-product claims with respect to the pre-breach communications of cybersecurity firms. For instance, when healthcare benefits provider Premera Blue Cross suffered a breach in 2015, it tried to shield its 2013 and 2014 technology audits from discovery on the grounds that they were privileged.[114] In rejecting these efforts, the court noted that the pre-breach audits were "normal business functions performed on a regular basis, to enable Premera to assess the state of its technology and security."[115] The mere fact that Premera delegated supervision of these business operations to counsel did not, the court emphasized, cloak them with confidentiality.[116]

C. Disclosure to Third Parties and Confidentiality Protections

Courts have long recognized that firms can waive both the attorney-client privilege and work-product protections by disclosing covered information to third parties. Concerning the attorney-client privilege, disclosure of privileged information to any third party can constitute waiver of privilege.[117] Some courts have even suggested that disclosure of otherwise-privileged information to employees outside of the firm's control group could result in waiver if those employees did

112. *CISA Tabletop Exercises Packages*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/cisa-tabletop-exercises-packages [https://perma.cc/W6RL-CN37].

113. *See Sedona Report*, *supra* note 24, at 37–38; *In re* Arby's Rest. Grp. Inc. Data Sec. Litig., No. 17-mi-55555, slip op. at 2 (N.D. Ga. Mar. 25, 2019) (holding that pre-breach communications between a technical consultant and counsel were privileged because the consultant was hired solely to aid the lawyer's analysis of Arby's compliance with the Payment Card Industry Data Security Standard).

114. *See In re Premera*, 329 F.R.D. at 666–67.

115. *Id.* at 666.

116. *Id.* at 667. The ruling did acknowledge that if "an attorney took the information from these documents and drafted a different document in preparation for litigation, that document would be protected." *Id.* It also noted that a "draft report sent to counsel seeking legal advice and input on the draft also would be privileged." *Id.*; *see also In re* Marriott Int'l, Inc. Customer Data Sec. Breach Litig., No. 19-MD-2879, 2021 WL 2660180, at *3, *6 (D. Md. June 29, 2021) (suggesting that privilege would not attach if Marriott shielded its investigation by having "attorneys engage in sham agreements with vendors on its behalf to perform work that was already to occur under pre-existing obligations," but rejecting this result because IBM's pre- and post-breach work were distinct).

117. *See, e.g.*, United States v. Deloitte LLP, 610 F.3d 129, 140 (D.C. Cir. 2010). *See generally* PRINCIPLES OF THE L., COMPLIANCE & ENF'T FOR ORGS. § 6.06 cmt. c (AM. L. INST., Tentative Draft No. 2, 2021) ("An organization that shares the specific content of the interviews — in writing or orally — would presumably waive the attorney-client privilege unless the sharing occurs under circumstances that support a selective waiver.").

not need to know the information for purposes of managing the firm's legal affairs.[118] By contrast, disclosure of materials protected by work product may not result in waiver unless those disclosures are made to adverse parties.[119] Concerning both attorney-client privilege and work-product doctrines, courts differ as to whether a disclosure to law enforcement or regulatory authorities of otherwise confidential information results in a waiver of those protections as to private litigants.[120]

These general rules, however, are subject to a host of important exceptions. For instance, the Cybersecurity Information Sharing Act of 2015 ("CISA") provides that disclosing information to certain Information Sharing and Analysis Organizations does not result in waiver of otherwise applicable attorney-client privilege or work-product protections.[121] Similarly, the Cyber Incident Reporting for Critical Infrastructure Act ("CIRCIA") of 2022 requires "critical infrastructure owners and operators" to report certain cybersecurity incidents to the federal government, and specifies that doing so will not result in a waiver of attorney-client privilege or work-product protections.[122] Finally, and perhaps most importantly, the "common interest" doctrine allows parties to share privileged information with a third party who has a common set of interests without jeopardizing the privilege.[123]

The common interest doctrine is particularly important in the cybersecurity setting when it comes to insurers. Because cyberinsurers often pay for a substantial fraction of their policyholders' breach response costs,[124] it would be sensible to think that they do indeed share a common interest in the breach response process with their policyholders. This intuition is supported by courts' general willingness to apply the common interest doctrine when policyholders disclose information related to the defense of a potentially covered claim to their liability insurers.[125] In both settings, insurers not only fund the underlying legal

118. *See Sedona Report*, *supra* note 24, at 22–23 (citing Verschoth v. Time Warner, Inc., No. 00-CIV-1339, 2001 WL 286763, at *3 (S.D.N.Y. Mar. 22, 2001)).

119. *See Deloitte*, 610 F.3d at 140.

120. *See Sedona Report*, *supra* note 24, at 23–24, 72–73; *In re* Columbia/HCA Healthcare Corp. Billing Pracs. Litig., 293 F.3d 289, 306 (6th Cir. 2002); *In re* Steinhardt Partners, L.P., 9 F.3d 230, 236 (2d Cir. 1993).

121. Cybersecurity Information Sharing Act of 2015, 42 U.S.C. §§ 1500–10.

122. Cyber Incident Reporting for Critical Infrastructure Act of 2022, 6 U.S.C. §§ 681–681g, 665j, 659.

123. *See* RESTATEMENT (THIRD) OF THE L. GOVERNING LAWS. § 76(a) (AM. L. INST. 1998).

124. *See* Sasha Romanosky, Lillian Ablon, Andreas Kuehn & Therese Jones, *Content Analysis of Cyber Insurance Policies: How Do Carriers Price Cyber Risk?*, 5 J. CYBERSECURITY 1, 5–6 (2019).

125. *See* RESTATEMENT OF THE L. OF LIAB. INS. § 11 (AM. L. INST. 2019); WILLIAM T. BARKER & CHARLES SILVER, PRO. RESPS. OF INS. DEF. COUNS. § 10.06 (2017).

activities about which disclosure is made, but also oversee the lawyers that coordinate these legal processes for the insured.[126]

Unfortunately, there remains some legal uncertainty regarding whether a policyholder may in fact share privileged information with its cyberinsurer without jeopardizing privilege. To date, no case has squarely addressed this issue.[127] And there are several potential distinctions between the cyberinsurance setting and the traditional liability insurance setting, where the common interest doctrine is relatively well established. Most fundamentally, a principal goal of breach response counsel is not to respond to a specific litigation threat (as with liability insurance), but instead to facilitate the provision of various first-party insurance benefits while limiting the risk of potential future litigation.[128] The lack of a specific lawsuit against the insured when breach counsel forms an attorney-client relationship with the insured arguably means that the breach counsel and policyholder are not as aligned in their interests with the insurer as is typical in the liability insurance setting.[129]

III. HARMFUL CONSEQUENCES: HOW LEGAL UNCERTAINTY DISTORTS AND UNDERMINES CYBERSECURITY

Courts and commentators have long recognized that the legal rules governing attorney-client privilege and work-product immunity could impact firms' cybersecurity efforts and the broader cybersecurity ecosystem.[130] To date, however, this possibility has remained largely speculative. For this reason, we endeavored to systematically study how firms' confidentiality concerns impact cybersecurity. To do so, we conducted semi-structured interviews with a broad range of professionals involved in cybersecurity preparedness and incident response.

These interviews paint a stark picture: confidentiality concerns dramatically impact each stage of cybersecurity preparation and incident response. In many cases, moreover, these concerns significantly undermine the capacity of firms to learn from and prevent future cyberattacks. Even more, confidentiality concerns impair the capacity of third

126. *See generally* KENNETH ABRAHAM & DANIEL SCHWARCZ, INSURANCE LAW AND REGULATION 615–51 (7th ed. 2020) (explaining the insurers' role in defending lawsuits).

127. The explanation for this trend may be that cyberinsurers accept lawyers' claims that disclosing post-breach information to insurers could result in a waiver of privilege, meaning that there have been few occasions to test it in court.

128. *See* Romanosky et al., *supra* note 124, at 5–6.

129. Divergent interests among liability insurers, policyholders, and insurance defense counsel are hardly uncommon. *See generally* Tom Baker, *Liability Insurance Conflicts and Defense Lawyers: From Triangles to Tetrahedrons*, 4 CONN. INS. L.J. 101 (1997); Charles Silver, *Does Insurance Defense Counsel Represent the Company or the Insured?*, 72 TEX. L. REV. 1583 (1994).

130. *See Sedona Report*, *supra* note 24, at 79–93; Kosseff, *supra* note 24, at 261–62.

parties such as insurers, regulators, and law enforcement to promote effective cybersecurity. These deleterious effects on cybersecurity have accelerated in recent years due to increasing legal uncertainty about whether firms' breach response efforts can be shielded from discovery through the attorney-client privilege or work-product protections.

We unpack these conclusions in several sections. First, Section A reviews our empirical methodology. Section B then describes the impact of confidentiality concerns on the documentation of cybersecurity incidents and the formal recommendations that cybersecurity firms develop for enhancing the network security of breached firms. Section C examines how these same concerns impact breached firms' contracts and communications with third-party cybersecurity firms. Finally, Section D looks at the impacts of confidentiality concerns on third parties, including insurers and regulators.

A. Empirical Methodology

Our research goal was not just to understand the law regarding the confidentiality of firms' cybersecurity efforts, but also to appreciate how these rules impact actors across the cybersecurity landscape.[131] Because no prior work had investigated this issue empirically, we conducted in-depth, semi-structured interviews with a broad range of actors across the cybersecurity ecosystem.[132] Such qualitative techniques are particularly appropriate for understanding complex interactions between legal rules and practice that have not previously been empirically studied.[133] Although interview-based methodologies cannot provide definitive evidence about how prevalent particular practices are or what causal pathways explain those practices, they can supply deeply textured information that illuminates the broader landscape and offer multiple potential avenues for future quantitative inquiry.[134] Qualitative methods are particularly useful for answering "how" research questions like those explored in this study (e.g., "how do concerns about privilege influence cybersecurity investigations?") and for building theories.

---

131. Legal academics have long understood that the law in books may diverge substantially from the law in practice. *See* Roscoe Pound, *Law in Books and Law in Action*, 44 AM. L. REV. 12, 15 (1910).

132. In recent decades, a broad range of influential legal scholarship has uncovered significant findings using similar interview-based methods. *See, e.g.*, John Rappaport, *How Private Insurers Regulate Public Police*, 130 HARV. L. REV. 1539, 1544 (2017); Tom Baker & Sean J. Griffith, *Predicting Corporate Governance Risk: Evidence from the Directors' & Officers' Liability Insurance Market*, 74 U. CHI. L. REV. 487, 487 (2007); Lisa Bernstein, *Opting Out of the Legal System: Extralegal Contractual Relations in the Diamond Industry*, 21 J. LEGAL STUD. 115, 157 (1992).

133. *See* Tom Baker, *Blood Money, New Money, and the Moral Economy of Tort Law in Action*, 35 LAW & SOC'Y REV. 275, 280 (2001) ("Talking and — more important — *listening* to lawyers in practice is an essential aspect of understanding the role of law in society.").

134. *See* Baker & Griffith, *supra* note 132, at 492.

We conducted sixty-nine semi-structured interviews lasting between thirty and sixty minutes each from 2020 to 2022.[135] We selected interview participants by contacting representatives from all ten law firms listed on more than two insurance panels in a study of twenty-four publicly available cyber insurance panels.[136] Additionally, we contacted representatives from law firms, insurers, and forensic investigation firms known for their expertise in cybersecurity incident response, as well as other professionals recommended to us by our interview subjects.[137] We consulted public lists of the leading "Big Law" firms with substantial practice areas in cybersecurity and emailed the attorneys who led those practices to request interviews.[138] We also interviewed lawyers from seventy percent of the law firms that have relationships with more than two major cyberinsurers, and forensic investigators from sixty-five percent of the cybersecurity firms with similar cyber-insurance relationships. We did not interview firms' internal general counsels, because these lawyers typically do not focus specifically on cybersecurity breaches.

All of the interviews were conducted remotely via videoconferencing software. The interviews were not recorded, but they all included at least two of the three authors, with one of the authors serving as a dedicated note-taker.[139] When conducting the interviews, we used a common set of high-level questions, which varied depending on the type of interview subject. We asked additional clarification questions based on the interviewees' responses.

After completing the interviews, we took several steps to ensure that our reporting accurately reflected interview subjects' statements. First, we developed a detailed summary of our findings and sent them to all interview participants, asking them if any of our conclusions were inconsistent with their impressions. This process predominantly

---

135. We obtained ethical approval for the interviews from one of the author's institutions, which included reviewing an initial version of the study's information sheet and interview script. All of the interview documentation quoted in this piece is on file with the authors.

136. *See* Woods & Böhme, *How Cyber Insurance Shapes Incident Response: A Mixed Methods Study*, *supra* note 51, at 14. An insurance panel is a group of attorneys that a liability insurer pre-approves to defend policyholders who are sued. *Id.* at 5.

137. We identified law firms focused on providing cybersecurity services but not represented on insurance panels by consulting public lists of top firms specializing in such areas. *See, e.g.*, *Cyber Law (Including Data Privacy and Data Protection)*, LEGAL 500, https://www.legal500.com/c/united-states/media-technology-and-telecoms/cyber-law-including-data-privacy-and-data-protection/ [https://perma.cc/5RAY-RQX5]. For each firm, we reviewed the professional biographies of lawyers in the relevant practice area to determine whether their practice included helping clients to manage cyber-incident response.

138. *See id.*

139. We did not audio record the interviews because early discussions revealed this would make participants uncomfortable or cause them to withdraw from the study. To mitigate this, we had a dedicated scribe on all calls. The scribes tried to record participants' responses word for word, especially core arguments. However, we inevitably failed to achieve perfect fidelity. Any inaccuracies are unlikely to impact results because we are not analyzing the choice of phrases but instead the high-level strategies that lawyers employ.

resulted in positive feedback while also producing several minor changes in how we reported the underlying data. Second, for the interviews of lawyers, which followed a stable set of topics, we quantitatively coded participants' responses to twenty-four specific questions. This data is reported in Appendix A. Doing so allowed us to confirm our broad impressions regarding the results and better understand the topics on which interview subjects offered divergent perspectives.

B. Impacts on Incident Documentation and Recommendations

Confidentiality concerns significantly impact documentation of firms' cybersecurity efforts and breaches. By far the most significant such impact involves cybersecurity firms' post-breach development of a final report or formal recommendations for enhancing network security. This is addressed in Subsection One. Subsection Two then turns to how confidentiality concerns impact the documentation of pre-breach cybersecurity efforts.

1. Documentation of Cyber-Incident Response

The most significant strategy that lawyers employed to protect the confidentiality of cybersecurity incident investigations was to limit the production of written documentation regarding how the breach occurred and how similar breaches could be prevented in the future. Every one of the twenty-three lawyers we interviewed said they did not always encourage cybersecurity firms to produce a final, written report detailing the findings of their breach investigations.[140] And about half of the lawyers we interviewed indicated that their standard practice was to direct the cybersecurity firm not to author such a report. Lawyers who centered their practice on breach response and received a significant amount of their work from insurers were particularly likely to insist that cybersecurity firms should typically not produce any final written report.

Several lawyers and forensic investigators suggested that different law firms approach oversight of incident response in very different ways, depending in large part on their business strategy and structure. Smaller firms focused largely or exclusively on cybersecurity incident response, received most of their business via referrals from insurance panels, and charged lower hourly rates for their services. In contrast, larger firms practiced in a number of different areas, typically charged

140. *See, e.g.*, *infra* notes 143–51 and accompanying text.

rates too high to be listed on insurance panels, and investigated a smaller number of breaches for long-term clients.[141]

The term "breach mill" was used to describe how law firms could run thousands of incident responses every year. This involved joining one or more cyber insurance panels that provide a steady stream of business, albeit at much lower hourly rates, and meeting this volume by pushing work down to associates. Such firms tended to see the legal strategy surrounding cyber-incident response as a commodity in which every firm followed the same protocol. This process was designed to maximize protections of privilege, such as by always hiring a new cybersecurity firm with whom the law firm had a good relationship and which often involved minimal documentation.[142]

The forensic investigators we interviewed also identified that their production of final reports had become less common in recent years.[143] Several forensic investigators said that the decision about whether to write a report varied by incident and law firm. One investigator estimated that counsel requested that they produce a formal report in "less than 5 [percent] of cases, because in such a report we would have to document all the screw ups."[144]

Lawyers generally explained their reluctance to direct cybersecurity firms to produce formal written reports by noting that this strategy minimized the risk that potentially damaging information about the client's security posture could be used against the client in a subsequent lawsuit. These lawyers frequently emphasized their lack of confidence in their capacity to shield such reports from discovery under attorney-client privilege and work-product protections following the 2020 *In re Capital One* and *In re Rutter's* cases.[145] Many of the lawyers opined

---

141. Some of the lawyers we spoke to charged $500 an hour, falling to as low as $300 for associates, while others were partners at elite law firms charging more like $1,500 hourly rates. Zoom Interview with Breach Att'y 13 (Jan. 7, 2022).

142. Several interviewees expressed the view that attorneys working at firms that center their business on incident response excessively push the importance of preserving privilege. Doing so, they claim, allows these attorneys to retain their control over the incident and their privileged place in regularly securing business. One lawyer said of breach-focused firms' approach to incident response, "There's no specialized attention, it's routine and formulaic," adding, "those firms are too mechanical and that's ok if it's not overly complex." Zoom Interview with Breach Att'y 1 (Feb. 3, 2022). Another lawyer at a large firm described the firms that focus exclusively on providing breach response via insurance panels as following a "cookie cutter" approach. Zoom Interview with Breach Att'y 16 (Jan. 5, 2022).

143. One forensic investigator said, "It used to be that every time we responded to a breach, a client wanted a report at the end of it . . . . There's just less reports written than there used to be. Only the most sophisticated clients are asking for reports these days and only for the most complicated incidents." Zoom Interview with Forensic Investigator 2 (Jan. 13, 2022).

144. Zoom Interview with Forensic Investigator 1 (Jan. 13, 2022).

145. *See supra* Section II.A (discussing *In re Capital One* and *In re Rutter's*). One attorney explained, "If I know there's likely to be litigation[,] we don't produce a report . . . . People will go to the mat to get the report so it's much easier to just say 'I'm sorry, we don't have one.'" Zoom Interview with Breach Att'y 14 (Jan. 6, 2022). Another said of the *In re Capital One* ruling: "[The courts] have jumped the fence and no longer respect privilege on the report,

that these cases were wrongly decided and injected substantial uncertainty into predicting when courts would treat forensic reports as privileged or otherwise nondiscoverable.

Even in instances when lawyers instructed a cybersecurity firm to produce a final report, they typically went to great lengths to shape that report. For instance, virtually every lawyer we interviewed indicated that such reports would be crafted jointly by lawyers and cybersecurity firms, with lawyers instructing cybersecurity firms to redraft language that they believed could be taken out of context to support liability.[146] A repeated request from lawyers was that the report only contain factual information.[147] Investigators also said that they avoided including any language in reports about breached firms' vulnerabilities in order to please lawyers and that they often faced pushback from lawyers about their wording in these reports.[148]

Some lawyers identified various situations in which they might ask a cybersecurity firm to produce a final report, notwithstanding their general inclination to avoid this result. For instance, an investigation describing an incident that occurred notwithstanding a firm's robust security protocols was more likely to result in a formal report. By contrast, several lawyers said they would be unlikely to ask for reports for cybersecurity incidents where a forensic investigation revealed that the victim organization had an extremely poor security posture, responded in especially ineffective or negligent ways, or was likely to be sued.[149]

---

therefore we're not creating the report." Zoom Interview with Breach Att'y 22 (Jan. 7, 2022). A third lawyer echoed this sentiment, saying "[s]ince [*In re Capital One*] I've not received a report, zero, because I tell them not to . . . . The trajectory of the law is doing a disservice to cybersecurity." Zoom Interview with Breach Att'y 12 (Jan. 7, 2022). A fourth attorney said, "I've started to advise against written reports. It was not our practice before [*In re Capital One*]. I'd say 75 [percent] of the time before Capital One we had written reports, now in 75 [percent] plus we do not." Zoom Interview with Breach Att'y 9 (Jan. 11, 2022).

146. One lawyer said, "We'll give instructions as to what we want to see in [the report] and what we don't want to see in there . . . . [W]e try to give guidelines like: no adjectives, no adverbs." Zoom Interview with Breach Att'y 3 (Jan. 20, 2022).

147. One attorney said he tries to avoid "gratuitous language like 'these are the best practices in information security.'" Zoom Interview with Breach Att'y 5 (Jan. 14, 2022).

148. A former investigator who now works for an insurance firm recalled an investigation that involved "two or three days going back and forth with the lawyers about specific wording in the report where they didn't want me to say that a specific server was vulnerable." Zoom Interview with Insurer 5 (Jan. 6, 2022). What some law firms viewed as "editoriali[z]ing," in other words, seemed to forensic investigators to be plain statements of the facts around vulnerabilities in a system. Zoom Interview with Breach Att'y 19 (Jan. 5, 2022).

149. According to one lawyer, "[T]here are times when the findings are just so bad that you don't want to reduce that to writing." Zoom Interview with Breach Att'y 11 (Jan. 11, 2022). Another said:

> The only times we do a full-fledged forensics report is if there's no personal information stolen that you need to disclose, it didn't affect anyone, then I would say let's get a full-fledged forensics report so that a year from now we can make sure we learned everything and implemented everything as a result of it because there's no risk anyone's ever going to see it because . . . it didn't affect anyone.

Additionally, some lawyers explained that they might ask for a final report for clients subject to expansive regulatory scrutiny to satisfy those regulators by showing that the firm had acted appropriately in response to a breach.[150] This type of nuance was more common among lawyers who worked for more high-profile law firms that were not included on insurance panels.[151]

Other lawyers explained that they would occasionally instruct cybersecurity firms to produce short executive summaries of their findings or other high-level final documents, such as stripped-down PowerPoint presentations or timelines of events.[152] Another approach is for external counsel to receive a final report and then write a second document summarizing this report that would be sent to the client. Such a document, because it was authored by a lawyer, would be much more likely to be treated as privileged, according to interviewees.[153]

Several lawyers were particularly focused on avoiding any written security recommendations from forensic investigators, either because those recommendations might not subsequently be adopted by the client or because they might imply that the cause of the incident was the lack of the recommended control.[154] Additionally, lawyers expressed

---

Zoom Interview with Breach Att'y 5 (Jan. 14, 2022).

150. One lawyer interviewed said that "oftentimes GDPR or HIPAA have a procedural requirement to document what was found, but we don't use the privileged report for those purposes, we make a separate report for that." Zoom Interview with Breach Att'y 3 (Jan. 20, 2022).

151. In the words of one breach attorney:

> [Very large firms] have a ton of people and they're cookie cutter. I end up having a lot of clients where [the firm] is foisted upon them by the insurer and then I check their work. They are hiring cannon fodder among young associates — you're gonna learn how to be a data breach investigator and that's all you're going to learn . . . . I do find there are certainly lesser known firms who are driven by the insurance. The people whose primary source of clients are the insurance relationships are lower rates, lower pedigree, it doesn't mean they aren't good at their jobs. But that's not who my firm is going to hire.

Zoom Interview with Breach Att'y 16 (Jan. 5, 2022).

152. One lawyer said there were three categories of report formats: "(1) only oral, (2) stripped-down [P]ower[P]oint, and (3) full reports." Zoom Interview with Breach Att'y 16 (Jan. 5, 2022).

153. One lawyer who took this approach further justified summarizing forensic reports in their own memos by claiming that doing this was necessary to make otherwise "incomprehensible" forensic reports understandable. Zoom Interview with Breach Att'y 6 (Jan. 14, 2022).

154. One lawyer said:

> A lot of times the [incident response] providers will say "we've got nine ideas for remediation" and we'll say, "that's great but don't put those in the report." . . . What we really don't want is a written report that says do these nine things and the client only does three of them and then there's another incident later on that would have been stopped by one of those things they didn't do.

Zoom Interview with Breach Att'y 3 (Jan. 20, 2022). Another lawyer explained, "[W]hen I become concerned is when the forensics team is producing a paper trail. Because then plaintiff

concern that generalized recommendations that were untethered to remediating a specific cybersecurity incident could jeopardize privilege claims by making it appear that the vendor's services were not genuinely limited to facilitating the lawyer's investigation, but were instead directed to serving the more general business needs of the client.[155]

Stakeholders expressed a wide variety of views on the impacts of instructing a cybersecurity firm not to produce a final report. Virtually all stakeholders identified a trade-off, acknowledging that the lack of documentation could cause long-term problems when reconstructing the incident to assess the long-term effectiveness of cybersecurity processes, facilitating a regulatory inquiry, or simply reconstructing the incident for internal purposes after time had passed.[156]

The forensic experts we interviewed were particularly concerned about the cybersecurity consequences of forgoing a final report. First, several experts suggested that the lack of a final report could have immediate negative impacts on the effectiveness of incident-response efforts for remediation.[157] Some of these consequences involved the ability of a cybersecurity firm to do its job effectively. For instance, the lack of a final report could limit accountability for deficiencies in the investigative process, inhibit efforts to reconcile potentially conflicting information discovered in the investigative process, and allow gaps in the investigative process to go unnoticed. As one former forensic investigator put it, "[T]here's a lot of information you can convey verbally[. B]ut when you have larger companies with bigger teams[, having that report] gives them such a better understanding of the weaknesses in their systems."[158]

The absence of a formal report could also impair the ability of internal firm personnel to understand how their networks were compromised and how that result could be prevented in the future.[159] Forensic

---

can say, 'your outside expert said you should do this, and you didn't so you were negligent.' So I don't want that in writing." Zoom Interview with Breach Att'y 7 (Jan. 13, 2022).

155. *See supra* Section II.A.1.c (noting that courts are less likely to treat a report as privileged when it includes recommendations for how firms can remediate cybersecurity failures). One lawyer said, "[A] lot of recommendations are marketing as much as anything — marketing for further services, often not tailored to the incident, often copy and pasted, sometimes even things [the client has] already done." Zoom Interview with Breach Att'y 19 (Jan. 5, 2022). Another echoed these concerns, saying, "For some firms, the recommendations are boilerplate long list that may not make sense in a particular context." Zoom Interview with Breach Att'y 4 (Jan. 6, 2022).

156. One attorney pointed out, "It's hard to keep track of very complex networks without writing things down." Zoom Interview with Breach Att'y 12 (Jan. 7, 2022). A forensic investigator also explained, "[*In re Rutter's* and *In re Capital One*] are making it so that clients are scared to have a good investigation or a report written so you don't get as good an investigation and you don't get proper mitigation." Zoom Interview with Forensic Investigator 2 (Jan. 13, 2022).

157. *See, e.g.*, Zoom Interview with Insurer 5 (Jan. 6, 2022); Zoom Interview with Forensic Investigator 2 (Jan. 13, 2022).

158. Zoom Interview with Insurer 5 (Jan. 6, 2022).

159. *See* Zoom Interview with Forensic Investigator 2 (Jan. 13, 2022).

investigators said it was often difficult to explain recommendations verbally, given recommendation complexity and nuance and the likelihood of employee turnover.[160] This concern that it was more difficult to provide cybersecurity guidance to clients in the absence of a written report was echoed not just by forensic investigators but also by some of the lawyers.[161]

Second, most of the forensic investigators we interviewed opined that the lack of final forensic reports could have damaging long-term consequences for breached firms. Because these firms have no written record of the findings of the investigation or the recommendations of the technical investigators, they have little ability to refer back to anything in later months or years if they want to assess whether they have made progress toward meeting those recommendations. Investigators also said they believed that the lack of documentation means that information technology ("IT") teams may struggle to advocate for resources from higher-level management because there is no record of the outside investigators recommending the security controls they wish to purchase and implement.[162] Such advocacy is much more difficult when recommendations are not included in a final report or even formalized in writing.[163] Additionally, investigators noted that the tendency for only more favorable or positive investigations to result in a report produces some bias in which incidents are documented, thus eroding the ability of organizations to learn from the incidents where it is essential they improve their security.

Lawyers expressed more limited concerns about the cybersecurity consequences to their clients of forgoing a written final report from cybersecurity firms. Most notably, many lawyers argued that communicating cybersecurity firms' security recommendations orally rather than

160. The investigator explained, "For continuity purposes, you can't assume the person you're talking to today is going to be employed tomorrow, and these are long-term plans. And I'm not going to sit there and read IP addresses — if you need to whitelist or blacklist these 7[,]000 IP addresses, you need that in writing." *Id.*

161. One attorney said he asked for written reports "not always, but more often than not." Zoom Interview with Breach Att'y 4 (Jan. 6, 2022). The attorney explained, "[S]ome lawyers say that's crazy. But I say they're nuts because they don't know what they're doing . . . I've asked opposing counsel for [Indicators of Compromise] and they won't share them. That is a detriment to the entire community. The only way companies can improve is sharing [Indicators of Compromise]." *Id.*

162. An investigator explained, "IT directors can strategically use forensics reports to win internal resources. But this doesn't happen and can't happen if I just deliver it to counsel . . . . [B]y the time it makes it to customers, it's probably not doing any good at that point." Zoom Interview with Forensic Investigator 6 (Jan. 4, 2022).

163. One investigator shared an anecdote in which the client's IT team had wanted to implement one of the investigator's recommendations, and so the vendor made it the highest priority recommendation in the report. Zoom Interview with Forensic Investigator 6 (Jan. 4, 2022). Formalizing recommendations in reports also allows lawyers to advocate for resources to adopt those recommendations by framing the issue in terms of compliance and legal risk. For example, one external counsel reported presenting recommendations at a board meeting. *Id.*

in writing was sufficient to ensure that clients received appropriate guidance.[164] However, several lawyers indicated that they did not believe oral briefings of security recommendations were sufficient.[165] A number of lawyers also indicated that, when it was important to document security recommendations, memos authored by lawyers that summarized these recommendations were sufficient.[166] However, forensic investigators noted that lawyers often made errors in communicating security recommendations to clients or else failed to fully communicate these recommendations, likening the process to a game of "telephone."[167]

2. Documentation of Pre-Breach Cybersecurity Efforts

While almost every lawyer and forensic investigator we interviewed said documentation of incident investigations was routinely limited due to confidentiality concerns, there were more mixed views on the documentation of pre-breach processes like risk assessments, penetration testing, and tabletop exercises. Consistent with the caselaw discussed in Part II, most lawyers said documentation resulting from such activities was difficult to shield from discovery in subsequent lawsuits.[168] Even the lawyers who indicated that they try to protect privilege for pre-breach materials also said they were uncertain of their ability to do so.[169]

Given these limited confidentiality protections, several lawyers said part of their role in overseeing pre-breach cybersecurity efforts was to prevent any audits or assessments that presented the client's security posture in a negative light.[170] These lawyers said they explicitly tried

164. *See, e.g.*, Zoom Interview with Breach Att'y 7 (Jan. 13, 2022); Zoom Interview with Breach Att'y 23 (Jan. 18, 2022).

165. Two lawyers interviewed said that they did direct forensic firms to include recommendations in the final reports issued to their clients. One of them explained, "If I were a judge, and there's no recommendations or report, then it would be a transparent effort to hide information from plaintiffs, it would suggest they're prioritizing litigation over acting responsibly." Zoom Interview with Breach Att'y 2 (Jan. 20, 2022). Another noted, "Verbal reports cover about 50% but those are usually to a very limited audience and they want to take it back to their entire IT team, so from our perspective the written recommendation is better." Zoom Interview with Breach Att'y 11 (Jan. 11, 2022).

166. *See, e.g.*, Zoom Interview with Breach Att'y 9 (Jan. 11, 2022).

167. *Id.*

168. *See supra* Section II.B (concluding that courts will rarely treat pre-breach cybersecurity efforts as privileged or covered by work-product immunity).

169. One attorney said, "We try [to protect confidentiality of pre-breach materials], but we also are candid that our ability to privilege [sic] this is unclear." Zoom Interview with Breach Att'y 7 (Jan. 13, 2022). Another said that having outside counsel contract with security vendors for pre-breach services "gives you a credible basis for refusing [to provide those materials to plaintiffs], but if [the plaintiffs] are committed and they press, then they are likely to prevail." Zoom Interview with Breach Att'y 22 (Jan. 7, 2022).

170. One lawyer said, "If there are gaps identified in the assessment we would rather not document those gaps in a way that could be used against [our client]." Zoom Interview with

to prevent risk assessment reports that showed significant or glaring vulnerabilities (e.g., color-coded with red labels or dramatic "high-risk" warnings).[171] They noted that such assessments were often exaggerated in their severity and could be used against firms in case of a later security incident that led to litigation.[172] Moreover, they often viewed these types of assessments as engineered to scare a company into purchasing the services of the firm that performed the assessment.[173] One attorney said they reviewed the outputs of pre-breach audits and assessments before sending them to a client and removed "unrealistic deadlines or dramatic language."[174] These types of edits suggest that concerns about the inability to cover pre-breach assessments under privilege may alter the tone and style of these assessments in ways that could undermine their effectiveness.

Although most stakeholders acknowledged the possibility that limited confidentiality protections could disincentivize firms from engaging in robust pre-breach cybersecurity efforts, they predominantly thought that this possibility was more theoretical rather than real. The benefits to firms of proactively limiting the risks of cyber intrusions or the consequences of such events dramatically outweighed the potential costs of documents produced during this process being used against those firms in subsequent litigation, in their view.[175] Some attorneys, however, expressed concerns that the lack of privilege might deter

---

Breach Att'y 3 (Jan. 20, 2022). Another said that security assessments were often "toned down" and particularly negative reports were never passed on to the client. Zoom Interview with Breach Att'y 13 (Jan. 7, 2022).

171. One lawyer said of pre-breach assessments:

> They're like RED RED RED RED. You look at the report and it's like a plaintiff's dream and of course [the security firm is] doing it because they want to get more work[,] but they structure it in this very alarming way to get more work . . . I had one recently where it was terrible and I just said to the forensics team, "we don't want a final report, just keep this in draft form."

Zoom Interview with Breach Att'y 14 (Jan. 6, 2022).

172. *Id.*

173. *See id.*

174. Zoom Interview with Breach Att'y 22 (Jan. 7, 2022).

175. One attorney said, "the odds of you suffering an incident and then the assessment finding something that caused the incident is very low . . . whatever the odds are, they're offset by the benefit in terms of improving cybersecurity posture." Zoom Interview with Breach Att'y 20 (Jan. 5, 2022). On the importance of proactive rather than reactive cybersecurity efforts, see CYBERRISK ALLIANCE, CYBERSECURITY RESOURCE ALLOCATION & EFFICACY INDEX Q-2 2020 REPORT 1 (2020), https://www.cyberriskalliance.com/wp-content/uploads/2020/08/CRAE-Index.pdf [https://perma.cc/J7ZQ-9AXH] (noting that firms are investing more in proactive rather than reactive cybersecurity efforts); Soumitra Sudip Bhuyan et al., *Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations*, 44 J. MED. SYS. 98, 102–04 (2020); Scott J. Shackelford, *Protecting Intellectual Property and Privacy in the Digital Age: The Use of National Cybersecurity Strategies to Mitigate Cyber Risk*, 19 CHAP. L. REV. 445, 459 (2016); Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEX. L. REV. 1533, 1561 (2010).

some clients from engaging in robust pre-breach security screening.[176] These concerns provide some support to the claim, expressed by others, that the privilege framework creates a "perverse incentive system" whereby "[a]ssisting attorneys in litigation receives more protection from discovery than developing technical remediation measures that are separate from legal strategies."[177]

C. Impacts on Incident Response Contracting and Communications

Lawyers' efforts to promote confidentiality not only significantly impact firms' documentation of their cybersecurity activities; they also shape the character and scope of incident-response processes. These effects are starkly visible in the procedures that firms and lawyers use to hire and direct cybersecurity firms. They are also present in the protocols that control communications among personnel at the cybersecurity firm, breached firm, and their lawyers.

1. Hiring Cybersecurity Firms to Conduct Cyber-Incident Response

Almost every lawyer we interviewed routinely advised their clients to contract with a cybersecurity firm in the aftermath of a breach through a tripartite agreement, which included the external law firm as a contracting party. Doing so, lawyers noted, was crucial to establishing that the breach investigation was being done to facilitate legal advice or in anticipation of litigation, such that attorney-client privilege or work-product protections would potentially attach.[178] One attorney said the *In re Capital One* ruling had changed their practice so that in some cases, now, the law firm is the sole party to retain the cybersecurity firm, rather than having a tripartite agreement. Additionally, that lawyer now recommends that payments to the cybersecurity firm come from the client's legal, rather than IT, budget.[179]

Lawyers also typically played a significant role in selecting the forensic investigation firm. This was particularly common for law firms specializing in breach response services and relying on cyberinsurers

176. The absence of privilege "is a disincentive and also a concern for candor," one lawyer said, adding, "[Y]ou never want to put in writing what the security system is like, but you also need candor to improve the system. And there is a risk that there won't be as much frank assessment, because that would turn into a roadmap for plaintiffs." Zoom Interview with Breach Att'y 7 (Jan. 13, 2022).

177. Kosseff, *supra* note 24, at 284.

178. *See supra* Section II.A.1.a (suggesting that courts strongly weigh which party hired a forensic firm in their work-product and privilege analysis).

179. *See* Zoom Interview with Breach Att'y 14 (Jan. 26, 2022); *see also supra* Section II.A.1.d (noting that some courts have indicated that it may be relevant to confidentiality considerations who pays for the forensic firm's services).

for their business.[180] Cyberinsurance carriers, more generally, were regarded by several interviewees as responsible for the central role that lawyers play in breach response, since many cyberinsurance policyholders are directed straight to a law firm by their carriers in the event of any kind of cybersecurity incident. "A lot of the 1-800 numbers on a cyberinsurance policy go directly to a law firm, they don't touch the insurer at all," one forensic investigator said.[181] They added that "privilege is one of the main ways that was sold."[182] Another forensic investigator indicated that their firm now routinely directs breach victims who contact them to go through a lawyer instead of working with the cybersecurity firm directly.[183]

Many lawyers identified a trade-off between retaining a technical firm that provided pre-breach cybersecurity services to assess an incident and hiring a new cybersecurity firm in the immediate aftermath of a potential breach. Several lawyers believed that hiring a new cybersecurity firm that did not have a pre-existing relationship with a client increased the chances that a court would deem that firm's work product to be privileged or otherwise shielded from discovery, often citing *In re Capital One* for this proposition.[184] This is because hiring a new cybersecurity firm clearly signaled that the firm's work was directed principally to assisting the lawyer in providing legal advice connected to an incident, rather than to providing services that the firm would require independent of legal issues. Lawyers also indicated that hiring a new cybersecurity firm was preferable because it eliminated the risk that the firm would downplay its own failures in investigating the root cause of a breach.[185] These views were particularly common among lawyers who worked at firms that specialized in breach response.[186]

---

180. Zoom Interview with Forensic Investigator 4 (Dec. 16, 2021) ("[The breach coaches are] now in charge of the case, [so] they get to decide who's going to handle the case, so they are key in who gets the business."); *see also supra* note 141 (describing the differences between law firms specializing in incident response).

181. Zoom Interview with Forensic Investigator 4 (Dec. 16, 2021).

182. *Id.*

183. Zoom Interview with Forensic Investigator 1 (Jan. 13, 2021).

184. One lawyer explained, "[I]f you really wanted to preserve privilege, then the investigation firm would be separate from the firm who conducts IR or pre-breach activities." Zoom Interview with Breach Att'y 2 (Jan. 20, 2022); *see also supra* Section II.A (explaining that some courts are likely to treat a firm that provides both pre-breach and post-breach services as providing business services in both settings, even if a new contract or SOW is created in connection with the breach).

185. One lawyer said, "[I]t's almost like an inherent conflict of interest to have the firm that did the security work investigate their own failure." Zoom Interview with Breach Att'y 3 (Jan. 20, 2022). Another lawyer added, "We work with companies that are doing incident response 24/7[. T]hey've got a very good formula for going through it, they don't turn over every single rock." Zoom Interview with Breach Att'y 11 (Jan. 11, 2022).

186. *See, e.g.*, Zoom Interview with Breach Att'y 3 (Jan. 20, 2022); Zoom Interview with Breach Att'y 2 (Jan. 20, 2022); s*ee also supra* notes 141–42 and accompanying text (referencing the types of breach coaches).

However, several forensic investigators, and some lawyers, said that hiring a new firm post-breach makes for a less efficient investigation. In part, this is because "the new investigator has to learn the client and the environment" at the same time that they are trying to understand the scope of the breach, according to one forensic investigator.[187] Lawyers' preference for hiring a new security firm can also lead to a lower quality investigation in the event that they select "some new fly-by-night incident responder," rather than retain a well-established cybersecurity firm.[188] This touched on a common theme across all interviews, namely that the perfect legal response was not well suited to the speed at which incident response was conducted in order to contain an active adversary.[189]

If an existing cybersecurity vendor was to be maintained, lawyers routinely attempted to create the appearance of discontinuity via contracting and relying on organizationally distinct units within the vendor. For example, most vendors separate their monitoring and threat detection teams from their incident response team, which means there can be discontinuity in terms of personnel engaged pre- and post-breach. Contracting and billing practices also provided this function.[190] In rare cases, the lawyer would pay the pre-existing forensic vendor directly and then bill the client for these expenses.[191]

In addition to selecting cybersecurity firms and formally contracting with them, lawyers also typically define the scope of the cybersecurity firm's role in breach response. Several lawyers indicated that after *In re Capital One* they more carefully specified in the tripartite

187. Zoom Interview with Forensic Investigator 2 (Jan. 13, 2022).

188. *Id.*

189. For instance, simply drafting and approving a tripartite agreement in the wake of an attack could sometimes delay incident response efforts, though some lawyers were willing to allow work to commence even while contract language was being formalized.

190. For example, it was common for lawyers to terminate the monitoring contract and sign a new agreement related to the incident, which would involve drafting a new SOW that made clear that the vendor was providing services directly to the attorney for purposes of facilitating the provision of legal advice. *See supra* Section II.A.1.b (indicating that some courts accept that a single security firm can provide business-oriented pre-breach services and legal-support post-breach services when the governing contracts so specify).

191. The vast majority of lawyers rejected the idea that it was common practice to conduct dual investigations in the aftermath of a breach, with one focused on understanding the root causes of an incident and potential security solutions, and the other intended solely to facilitate the efforts of the company's lawyers. *See In re* Target Corp. Customer Data Sec. Breach Litig., No. 14-2522, 2015 WL 6777384, at *2 (D. Minn. Oct. 23, 2015) (holding that a forensic report prepared for the benefit of lawyers was privileged where a separate report was conducted for business purposes); Reynolds & Kim, *supra* note 11, at 7 (suggesting that firms should employ a dual-track investigation to increase confidentiality assurances). Instead, when a dual-track investigation does occur, it is usually not because of privilege considerations at all, but because two different parties are potentially impacted by a breach and have an interest in understanding their exposure. *See* Reynolds & Kim, *supra* note 11, at 7. Notably, a dual-track investigation was conducted in the case of the Target breach because the payment card brands required an independent investigation. *See infra* Section III.D.3.

agreement the precise services that the cybersecurity firm would provide to support the lawyer's work.[192] Forensic investigators indicated they were wary of suggesting additional tests or investigations to clients beyond those that the lawyers who hired them requested.[193] These dynamics were particularly stark as to the specialized breach-focused law firms listed on insurance panels.[194] Because these firms now control a large volume of investigations, a few investigators pointed out that their business relied heavily on keeping those specific law firms happy.[195] As a result, as one prominent lawyer at a firm focused on breach response noted, "when we say jump, [the cybersecurity firms] say 'how high?'"[196] Several forensic investigators also expressed concern that lawyers' primacy in defining the scope of their services could undermine cybersecurity.[197]

2. Communications During Cyber-Incident Response

Lawyers' importance in breach response extended well beyond the contracting process; lawyers also routinely coordinated communication flows among cybersecurity firms and clients throughout the breach response process. Lawyers often did so by establishing detailed communication protocols, which they distributed at the outset of an incident response process. They varied as to how much they attempted to limit communications between the forensic vendor and the client. At the most extreme end of the spectrum, all emails and calls had to involve

192. Zoom Interview with Breach Att'y 7 (Jan. 13, 2022) ("[T]here is more of an effort to try to define legal purposes in [the] SOW to address some of the language in capital one and Cargill case and make sure that [the contract contains] legal spin [in the] SOW . . . ."); *see also supra* Section II.A.1.f (indicating the relevance of the services provided and content of SOW to attorney-client privilege and work-product protections).

193. An investigator said that new case managers at their firm are trained to pay attention to what the lawyer wants more than the demands of the actual breached client. "For me the breach coach is the most important client," that investigator explained. Zoom Interview with Forensic Investigator 4 (Dec. 16, 2021). Another investigator said, "[W]e say that the counsel is our client and the counsel has their client, which we call client's client." Zoom Interview with Forensic Investigator 2 (Jan. 13, 2022).

194. *See, e.g.*, Zoom Interview with Forensic Investigator 4 (Dec. 16, 2021) ("Another thing is there's no upselling. We have another division, recovery and remediation, they can help you get back up and running . . . if you try to upsell on a scoping call you won't be getting the next call that day.").

195. One forensic investigator explained, "[Y]ou are . . . working for the lawyers as much, if not more than, you are working for the client. You're generally going to be a lot more afraid of the lawyers than the client." The investigator added, "The more you upset [the law firms] the more devastating impact it will have on your business." Zoom Interview with Forensic Investigator 3 (Dec. 14, 2021).

196. Zoom Interview with Breach Att'y 17 (Jan. 5, 2022).

197. One investigator said, "[I]f we're hired by a law firm, then we're going to do the project according to their [SOW] and scope of work. If it appears the scope is expanding, then we'll bring it to the law firm, but we let them decide if the scope should expand . . . ." Zoom Interview with Forensic Investigator 1 (Jan. 13, 2022).

external counsel.[198] Generally, most lawyers made some concessions when it came to vendors requesting access to the client's systems for investigative purposes or other purely technical or coordination matters.[199] The practical demands of carrying out a large-scale investigation generally do not allow for prohibiting all written communication or channeling everything through the law firm, most lawyers said.[200] The crucial communications that lawyers wanted to be involved in and preferred not to have put in writing were any findings that might point to mistakes or security failings on the part of the client.[201] Forensic investigators also said they had learned to be careful about what kinds of findings they put in writing.[202]

Lawyers explained their efforts to control communication flows during the incident response process in two ways. First, lawyers often emphasized that involving them in communications helped facilitate assertions of privilege or work-product immunity by demonstrating that they, rather than the breached firm, were directing the efforts of the cybersecurity firm.[203] Second, fearing that such preliminary documents might not be protected by privilege, lawyers often noted that initial speculation or hypotheses by technical investigators regarding an

198. For instance, one lawyer said, "For emails, counsel must always be CC'd . . . all written communications must include counsel, there's no exception. With phone calls, any status updates or conclusions need to have counsel on the call." Zoom Interview with Breach Att'y 1 (Feb. 3, 2022).

199. One lawyer said:

> We tell forensics firms that they can have direct communications with the client, but those communications are limited in scope — logistical or simple requests don't need to go through me. But, if there is ever discussion of substantive questions involving the data or vulnerabilities on the network, or talk about observations you're making . . . then I need to be part of those discussions.

Zoom Interview with Breach Att'y 23 (Jan. 18, 2022).

200. One lawyer explained, "We don't go so far as to say we don't let anyone send any email or we have to be involved in every single discussion because that's not practical, [sic] we'll never get done with anything." Zoom Interview with Breach Att'y 3 (Jan. 20, 2022). Another said that micromanaging communications could slow down the investigation and have adverse consequences for the remediation process. *See* Zoom Interview with Breach Att'y 6 (Jan. 14, 2022).

201. One lawyer said, "If the consultant is trying to get logs from IT people, we don't need to be on those calls, that's just logistical planning. Once conversations about where the firewalls were set up and how things were configured begin happening, we need to be involved in those conversations." Zoom Interview with Breach Att'y 15 (Jan. 5, 2022).

202. One investigator said:

> [Y]ou never opine on whether [the client has] good or bad data security. If you get on a scoping call with a client and they don't have multifactor authentication enabled, or their password was passw0rd with a zero, you never chastise them, you never comment, especially in writing, on how good their data security is. Because if all the emails get out in discovery then you've set up your client for failure.

Zoom Interview with Forensic Investigator 4 (Dec. 16, 2021).

203. *See supra* Section II.A.1.b (showing that courts often examine who is directing the cybersecurity firm in practice when evaluating claims of attorney-client privilege or work-product immunity).

incident often are not ultimately supported by the evidence as a whole.[204] Lawyers also repeatedly observed that technical investigators can frequently go beyond documenting facts to opining about the incident and breached company in ways that are inconsistent with their intended role.[205]

In addition to limiting how employees of breached firms and forensic investigators communicated, lawyers also exercised significant control over which employees of these firms were involved in communications. Most lawyers strictly limited high-level strategic communications to a "control group" containing only the key decision makers at the client firm.[206] These lawyers explained that doing so helped substantiate later assertions of attorney-client privilege or work-product immunity by helping frame cybersecurity firms' efforts as facilitating the provision of legal rather than business services to the impacted firm.[207]

Several forensic investigators indicated that these restrictions on the manner of communication and the individuals who could be included in communications impaired their ability to conduct effective investigations.[208]

---

204. For example, one lawyer reported how the IT director's machine had been compromised and the CEO immediately concluded that was the attack vector. Zoom Interview with Breach Att'y 12 (Jan. 7, 2022). Further investigation using timestamps revealed that the incident pre-dated the IT director's machine being compromised. *Id.*

205. One lawyer shared an anecdote in which a preliminary report stated the victim firm had "a pervasive culture of non-compliance." *Id.* Others implied that technical investigators were prone to "editoriali[z]e" and go beyond the bare facts. Zoom Interview with Breach Att'y 19 (Jan. 5, 2022). Limiting documentation preemptively addressed this problem. *Id.*

206. Zoom Interview with Breach Att'y 7 (Jan. 13, 2022). To the extent that information from additional employees was needed to facilitate the investigation, this information was gathered from that employee, who would then not remain part of the broader investigative effort. Zoom Interview with Breach Att'y 18 (Jan. 5, 2022). This meant that throughout the investigations those employees with the most technical knowledge of the breached organization's systems would often be asked to leave calls as soon as they had relayed needed information and were not included in many of the broader discussions about the incident. *See id.*

207. *See supra* Section II.A.1.g (noting that courts evaluating privilege and work-product immunity claims often consider the extent to which a cybersecurity firms' conclusions were widely disseminated at the impacted firm).

208. One investigator noted that attorney-client privilege "slows communications at every level" during an investigation. Zoom Interview with Forensic Investigator 3 (Dec. 14, 2021). Another echoed that sentiment, explaining, "[I]f you have a request for information, you need to go through lawyers to ask for that information, and then they would go to the client." Zoom Interview with Forensic Investigator 1 (Jan. 13, 2022). That investigator added that these delays can be critical because "[a]ll of these investigations are hugely time sensitive. Everything is changing constantly. And in lots of situations the volatile evidence that might be associated with a breach situation might not even exist by the time you finish monkeying around with the lawyer." *Id.*

D. How Confidentiality Concerns Impact Third Parties

Restrictions on the documentation and scope of a breach investigation do not just affect the victim of that breach and their ability to remedy their security posture. Various third-party stakeholders may also be interested in the results of an investigation. Yet virtually all such stakeholders we spoke to routinely said that they had trouble procuring relevant information related to cybersecurity incidents from the lawyers overseeing these investigations. Most of the lawyers interviewed acknowledged that they tried to limit any information about breaches shared with third parties, fearing that it could constitute a waiver of privilege or work-product immunity.[209] Lawyers also expressed concerns that sharing information could result in that information harming their clients in other ways, such as by being leaked to the public, forming the basis for a denial of insurance coverage, triggering a regulatory investigation, or increasing the costs of an audit. We elaborate on these conclusions below, focusing on four categories of third-party stakeholders: (1) insurers, (2) regulators and law enforcement agencies, (3) auditors and payment card counsel, and (4) supply chain partners.

1. Insurers

Insurers providing coverage for cybersecurity incidents have numerous potential reasons for requesting a forensic firm's investigative findings. Although some of these reasons have only a tangential relationship to cybersecurity,[210] others have potentially significant cybersecurity implications. Most importantly, access to forensic firms' breach reports or related materials could help cyberinsurers limit the risk of a breach through improved underwriting, targeted discounts, and various other insurer loss prevention strategies.[211] Indeed, the prospect of such insurer-driven enhancements to cybersecurity has been much

---

209. *See supra* Section III.C.2; *see also* Richard L. Marcus, *The Perils of Privilege: Waiver and the Litigator*, 84 MICH. L. REV. 1605, 1606 (1986) ("[E]normous energy can be expended to guarantee that privileged materials are not inadvertently revealed in discovery . . . .").

210. For instance, forensic reports or related materials could help insurers to deny claims when policyholders made material misrepresentations in their applications for coverage. *See* ABRAHAM & SCHWARCZ, *supra* note 126, at 11–36. Information from cybersecurity firms could also potentially be useful in administering claims.

211. *See* ERIN KENNEALLY, HIDING IN PLAIN SIGHT: TOWARDS NOW-GEN CYBER RISK UNDERWRITING, GUIDEWIRE WHITE PAPER 2 (2021), https://www.the-digital-insurer.com/wp-content/uploads/securepdfs/2021/09/1834-GuidewireCyenceRiskHidingInPlainSight.pdf [https://perma.cc/BTP3-YJ7W] (arguing that post-incident digital forensic reports offer important data for improving cyberinsurance underwriting that cyberinsurers have ignored). *See generally* Abraham & Schwarcz, *supra* note 26, at 20–35 (cataloging ways that insurers can potentially reduce the risk of loss); Omri Ben-Shahar & Kyle D. Logue, *Outsourcing Regulation: How Insurance Reduces Moral Hazard*, 111 MICH. L. REV. 197 (2012).

touted by the insurance industry and commentators,[212] even though evidence of this effect is quite limited.[213] Access to post-breach forensic materials could also help cyberinsurers monitor the activities of the third-party service providers whose costs they pay, including breach coaches and forensic firms. Enhanced monitoring of this type could improve the efficiency and effectiveness of breach response.[214]

In reality, insurers virtually never receive any written materials from the forensic firms that investigate covered breaches. Both lawyers and insurers said in interviews that lawyers routinely limit the information from forensic firms regarding a cyber incident that is shared with insurers.[215] And all of the stakeholders we spoke to indicated that to the extent that final reports are produced by forensic vendors, they are almost never shared with insurers.[216] Instead, most lawyers explained that they will generally have phone calls with insurers during which time they will only answer factual questions regarding the scope of the intrusion and the response to date.[217]

Lawyers justified these limitations on the information that they provide to insurers regarding forensic investigations by arguing that they are necessary to prevent waivers of potential confidentiality protections. Although a number of lawyers opined that sharing documents with insurers, including a final report, would likely not result in a

---

212. *See, e.g.*, Jay P. Kesan & Carol M. Hayes, *Strengthening Cybersecurity with Cyber Insurance Markets and Better Risk Assessment*, 102 MINN. L. REV. 191, 194 (2017) (calling for insurers to protect their profitability through comprehensive data assessments); Shauhin A. Talesh, *Data Breach, Privacy, and Cyber Insurance: How Insurance Companies Act as "Compliance Managers" for Business*, 43 LAW & SOC. INQUIRY 417 (2018); Baker & Shortland, *supra* note 14; Jan Martin Lemnitzer, *Why Cybersecurity Insurance Should be Regulated and Compulsory*, 6 J. CYBER POL'Y 118, 118 (2021). *But see* Kyle Logue & Adam Shniderman, *The Case for Banning (and Mandating) Ransomware Insurance*, 28 CONN. INS. L.J. 247, 293–315 (2021) (describing, and ultimately rejecting, insurers' arguments that insurers' pre- and post-breach services reduce the likelihood and severity of a ransomware attack).

213. JOSEPHINE WOLFF, CYBERINSURANCE POLICY: RETHINKING RISK IN AN AGE OF RANSOMWARE, COMPUTER FRAUD, DATA BREACHES, AND CYBERATTACKS 172–77 (2022); Shauhin A. Talesh & Bryan Cunningham, *The Technologization of Insurance: An Empirical Analysis of Big Data and Artificial Intelligence's Impact on Cybersecurity and Privacy*, 5 UTAH L. REV. 967, 975 (2021); JAMIE MACCOLL, JASON R. C. NURSE & JAMES SULLIVAN, CYBER INSURANCE AND THE CYBER SECURITY CHALLENGE, at vii (2021), https://rusi.org/explore-our-research/publications/occasional-papers/cyber-insurance-and-cyber-security-challenge [https://perma.cc/FLE4-BQDQ].

214. *See* Abraham & Schwarcz, *supra* note 26, at 251–53 (emphasizing that insurers have a particularly significant role to play in loss prevention efforts after a loss occurs due to the enhanced risk of moral hazard).

215. *See supra* Section III.C.2; Zoom Interview with Insurer 4 (Mar. 14, 2022).

216. *See supra* Section III.C.2; Zoom Interview with Insurer 1 (Jan. 20, 2022); Zoom Interview with Insurer 2 (Jan. 14, 2022); Zoom Interview with Insurer 3 (Jan. 13, 2022); Zoom Interview with Insurer 4 (Mar. 3, 2022); Zoom Interview with Insurer 4 (Jan. 6, 2022).

217. One insurance broker said that insurers often received information from lawyers via PowerPoint slides; lawyers were unwilling to provide copies of slides to the insurers or even allow them to take photos or screenshots of them during presentations. Zoom Interview with Insurer 4 (Mar. 3, 2022).

waiver of privilege under the common interest doctrine,[218] they generally argued that this risk was too high to warrant disclosure. In doing so, they emphasized that the issue was not yet tested in court and might depend on which jurisdiction adjudicated the matter.[219] Some lawyers also suggested they resisted providing documents regarding a cybersecurity intrusion because an insurer could use these materials to deny coverage or raise premiums.[220]

Cyberinsurers typically explained their willingness to accept this state of affairs by emphasizing that they cover not only the immediate expenses to policyholders of incident response but also any costs associated with subsequent litigation involving an intrusion, including any settlement or judgment.[221] For that reason, waiver of legal protections would harm insurers just as much, if not more, than the breached policyholder. Additionally, several lawyers, forensic investigators, and insurers said they thought that insurers had thus far been hesitant to demand information produced by cybersecurity firms because they could lose business as a result.[222]

Several insurers expressed frustration at how uninformative the oral information they were able to get from lawyers and clients was with respect to improving their underwriting models or pursuing broader loss prevention efforts. Insurers said that in many cases, the information conveyed on these calls was inaccurate, in part because it was not communicated directly by the cybersecurity firm that did the underlying work.[223] Even in cases when the information that is shared is accurate, it is typically not detailed enough, insurers explained, to help them understand how the accuracy of their underwriting models could be improved.[224]

While most respondents believed insurers could learn from detailed written information produced by cybersecurity firms, very few

---

218. *See supra* Section II.C (suggesting that disclosure to a cyberinsurer of a cybersecurity firm's breach report would likely not constitute waiver, but that the law on this point remains unclear).

219. *See supra* Section II.C.

220. *See, e.g.*, Zoom Interview with Breach Att'y 1 (Mar. 3, 2022). It is not perfectly clear whether it is ethical for lawyers to limit the availability of information to insurers on this basis; to the extent that breach response lawyers have an attorney-client relationship with both the cyberinsurers that pay them and the policyholders who receive these services, they cannot properly make decisions that advantage the policyholder at the expense of the insurer. *See* WILLIAM T. BARKER & CHARLES SILVER, PRO. RESPS. OF INS. DEF. COUNS. § 4.04 (2012).

221. Romanosky et al., *supra* note 124, at 6.

222. *See, e.g.*, Zoom Interview with Breach Att'y 6 (Jan. 14, 2022); Zoom Interview with Forensic Investigator 2 (Jan. 13, 2022); Zoom Interview with Insurer 4 (Mar. 3, 2022). *But see* Zoom Interview with Breach Att'y 5 (Jan. 14, 2022) (articulating how some insurers want to know the attack vector of a breach).

223. One insurer said, "[T]here is so much confusion in this call — it's a game of telephone. The forensic firm tells the breached firm who goes to counsel, it's all confused and jumbled. It's hard to get straight answers to simple questions." Zoom Interview with Insurer 1 (Jan. 20, 2022).

224. *Id.*

had experience of them doing so. Insurance personnel we interviewed often expressed interest in being able to access and learn from forensic reports, or use them for underwriting and pricing policies.[225] This was particularly true for interviewees working in underwriting; by contrast, insurance employees who worked on claims indicated less interest in acquiring these materials.[226] Some interviewees also acknowledged that the insurance industry was still figuring out how best to collect data about cybersecurity incidents and what types of information to request.[227] "[I]n most cases [insurers] don't know how to read a forensic report and how to react to it," one insurer explained.[228] "[I]nsurers aren't clamoring for it because they don't know what to do with it."[229] Still, the insurer added, those reports are useful to the carriers with technical expertise who are trying to understand what risk drivers they should be looking for in policyholders and how to "sharpen our underwriting."[230] One lawyer expressed a similar sentiment, noting that the risk models used by insurers were improving and that studying forensic reports was a part of this process.[231]

Given the potential value to insurers of forensic reports and the legal uncertainty regarding whether such disclosure would waive confidentiality protections, it is perhaps not surprising that some interviewees indicated that practices on this issue are in flux. We heard isolated anecdotes of insurers demanding forensic reports as a condition of payment.[232] And one insurance underwriter shared with us that an insurer had drafted new language for its insurance policy that required

---

225. Zoom Interview with Insurer 5 (Jan. 6, 2022); *see also* KENNEALLY, *supra* note 211, at 2 ("Digital forensics & incident response (DFIR) data about incident attack vectors and controls deficiencies collected at the backend of an incident (during the claims phase) will evolve the quality of risk correlation and causation and enrich the frontend underwriting of cyber risk.").

226. Zoom Interview with Insurer 1 (Jan. 20, 2022). This suggests that forensic reports may not, in fact, be terribly useful for administering claims or perhaps even for insurer monitoring of lawyers and forensic firms. *See supra* text accompanying notes 210–14 (describing these potential uses of information from forensic firms).

227. As one insurer put it, "Every carrier is dying for data, they just don't know what data they need." Zoom Interview with Insurer 5 (Jan. 6, 2022).

228. Zoom Interview with Insurer 3 (Jan. 20, 2022).

229. *Id.*

230. *Id.* One underwriter said that because so little information about investigations was shared by the lawyers overseeing incident response, insurers often had to rely on their instincts to guide their underwriting more than empirical data. "When we got our shirts handed to us by ransomware in 2020, we overhauled our ransomware underwriting model and strategy . . . . But, candidly, it was from my understanding and not from real data," the underwriter said. Zoom Interview with Insurer 1 (Jan. 20, 2022).

231. Zoom Interview with Breach Att'y 13 (Jan. 7, 2022).

232. We heard one anecdote in which a foreign insurer refused to pay a claim unless the forensic report was shared. *See* Zoom Interview with Breach Att'y 19 (Jan. 5, 2022). Under this threat, the lawyer and client shared the forensic report. *See id.* Another lawyer reported that insurers requested the report for claims in the millions of dollars but not for smaller claims. Zoom Interview with Breach Att'y 13 (Jan. 7, 2022).

insureds to provide the insurer with all reports produced by vendors.[233] That insurer is not pushing this form yet and is still introducing it to the market, the underwriter said, but it suggests that insurers may be reconsidering whether they want to apply more pressure to law firms and policyholders to share incident investigation findings with them.[234] Several interviewees also said that the current challenging market for cyberinsurance is changing insurers' calculations on these issues,[235] especially since insureds who resist sharing information from cybersecurity firms may be relatively risky.[236] Yet another forensic investigator noted that one insurer is even considering cutting out lawyers from the initial breach response process altogether in order to reduce costs;[237] doing so, of course, would completely eliminate any claim of privilege and hence that barrier to sharing information.[238]

In addition to demanding access to forensic information as a condition of claims payment, some insurers have attempted alternative strategies to acquire better information about their policyholders' breaches. For instance, one insurer regularly conducted "post-mortem" discussions after claims payments were made, on the theory that clients would be more forthcoming if they did not have to worry that doing so would result in a claim's denial.[239] However, the underwriter suggested that these efforts often failed to result in clients or the lawyers being forthcoming, even though this can and did result in the insurer not renewing the policy.[240]

Several stakeholders noted that lawyers often faced significant conflicts of interest in navigating these insurance-related issues. Lawyers who did not depend on insurers to refer cases to them had some freedom to push back against insurers' requests for information from cybersecurity firms.[241] Other lawyers who derived a substantial amount of their work from insurers often felt less freedom to push back against

---

233. Zoom Interview with Insurer 1 (Jan. 20, 2022).

234. *Id.*

235. Zoom Interview with Insurer 4 (Mar. 3, 2022); *see also* Tom Johansmeyer, *The Cyber Insurance Market Needs More Money*, HARV. BUS. REV. (Mar. 10, 2022), https://hbr.org/2022/03/the-cyber-insurance-market-needs-more-money [https://perma.cc/7NRV-EFGS] (explaining that the cyber insurance market has become "less enticing" for insurers).

236. One insurer said, "We do think about moving to a policy where it's more mandatory: you will share these details to obtain coverage . . . . Right now it's very much 'oh, you've got a forensic report? Great, would you share it with me?'" Zoom Interview with Insurer 4 (Mar. 3, 2022).

237. Zoom Interview with Forensic Investigator 4 (Dec. 16, 2021) ("[L]awyers have been in the drivers' seat from the beginning[,] but the reversal is just starting where insurers are asking if response firms can be the first call.").

238. *See supra* Section II.A.

239. Zoom Interview with Insurer 1 (Jan. 20, 2022).

240. *Id.*

241. *See, e.g.*, Zoom Interview with Breach Att'y 7 (Jan. 13, 2022) ("My experience is that insurers understand privilege issue and will back off. But they will also back channel me when I'm on the panel. When I'm on panel and breach coach. And in that setting, insurer will backchannel. This is [sic] huge ethical conundrum when representing client [sic] . . . .").

insurer demands for information or resistance to paying for certain services.[242]

2. Regulators and Law Enforcement

Respondents reported receiving requests from a number of regulators in the aftermath of a cyber incident. As with other third parties, lawyers often went to great lengths to limit the information they provided in response to such requests. One law firm said they never released documents and instead told the regulator they would provide answers to any question orally.[243]

Other respondents tailored the strategy to the regulator. One lawyer said that he always complied with requests from the Securities and Exchange Commission because the harm of damaging a relationship with the agency, whom the client dealt with in other contexts, outweighed the risks of waiving privilege.[244] Similarly, another lawyer indicated that sharing information with regulators of firms in the healthcare industry, where privacy is heavily regulated, was particularly important.[245] In contrast, many lawyers stated it was not worth complying with the Federal Trade Commission requests because that agency is either understaffed and unable to prosecute, or they decide to prosecute and hammer firms regardless of their level of cooperation.[246]

Consistent with these regulator-specific approaches taken by lawyers, the government regulators we interviewed expressed varying confidence levels in their ability to obtain information about cybersecurity incidents from breached firms. One said they were usually able to

242. *See, e.g.*, Zoom Interview with Forensic Investigator 4 (Dec. 16, 2021) ("[The breach coaches' real] client is the insurers — those guys are going to send 50–60 cases a week to these firms that they love. So the real loyalty lies with the insurer. As far as I know, every breach coach understands that and does not send data back to the insurer.").

243. Another lawyer, who said he was unique among the partners of his own firm, instead prioritized communicating with regulators. Zoom Interview with Breach Att'y 16 (Jan. 5, 2022). From his perspective, it was important to show the regulator that the incident was investigated, fixed, and steps were taken to improve in the future. *Id.* The benefits from doing so outweighed the risk in terms of waiving privilege. *Id.* However, he said this advice was specific to regulated industries. *Id.*

244. Zoom Interview with Breach Att'y 13 (Jan. 7, 2022).

245. Zoom Interview with Breach Att'y 16 (Jan. 5, 2022); *see also* Derek Mohammed, Ronda Mariani & Shereeza Mohammed, *Cybersecurity Challenges and Compliance Issues Within the U.S. Healthcare Sector*, 5 INT'L J. BUS. & SOC. RSCH. 55, 64 (2015) (discussing the unique privacy focus in healthcare regulation).

246. Zoom Interview with Breach Att'y 13 (Jan. 7, 2022). Various academics have also criticized the FTC's approach to cybersecurity on similar grounds. *See, e.g.*, Justin Hurwitz, *Data Security and the FTC's UnCommon Law*, 101 IOWA L. REV. 955, 980–1017 (2016) (arguing that the FTC's common law approach to data security regulation results in unsound legal principles); Michael D. Scott, *The FTC, the Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?*, 60 ADMIN. L. REV. 127, 143–44 (2008) (suggesting that the FTC had exceeded its authority in the past by taking action against victims of cybercrime who did not engage in meaningful wrongdoing).

schedule phone calls with the law firms overseeing the incident-response process and often demanded that IT representatives from the breached firm also join the call to answer questions about the specifics of the breach.[247] This regulator also said that they were rarely able to obtain reports but often did not need them in order to establish whether there had been a legal violation.[248] Another regulator pointed out that the perception of many lawyers that "once you share with one branch of government, you share with all of them" hindered the ability of government agencies to collect information about cybersecurity incidents.[249] By contrast, a prominent state insurance regulator reported that they were typically able to compel companies that had themselves experienced breaches to share information about the incidents because they could credibly threaten to revoke an insurer's license to do business or otherwise impose significant consequences if it refused to comply.[250]

Most lawyers expressed a willingness to cooperate with law enforcement agencies by sharing oral information about a breach. Several emphasized that the Federal Bureau of Investigation, in particular, understood the risk of waiving privilege and was comfortable with verbal updates.[251] Some lawyers, however, were more cautious about sharing information with law enforcement. For instance, one lawyer noted that some agencies, including the FTC, often explicitly asked for anything that had been shared with another government entity.[252] Such strategies, they said, could undermine their ability to share freely with law enforcement, as doing so could require them to share all the same materials with the FTC.

3. Auditors and Payment Card Counsel

External auditors commonly requested documents about breach investigations, including any final reports. Respondents were more likely to refuse such requests compared with the other third-party stakeholders identified in this Section, emphasizing the potential that doing so

247. Zoom Interview with Regulator 2 (Jan. 19, 2022).

248. This regulator explained, "The executive summary is fine for our purposes . . . . We sort of half-heartedly ask on these calls — and most of the time I don't — is there a report? But it's evolved to a point where most of the time they're not writing a report, and that's a shame." *Id.*

249. Zoom Interview with Regulator 1 (Jan. 18, 2022). The regulator also said, "If someone delivers us something with caveats — don't share, or don't share without approval — then we try to honor those[,]" adding that such caveats were often attached to information provided by the private sector to his agency. *Id.*

250. Zoom Interview with Regulator 2 (Jan. 19, 2022).

251. *See* Zoom Interview with Breach Att'y 11 (Jan. 11, 2022); Zoom Interview with Breach Att'y 8 (Jan. 12, 2022).

252. Zoom Interview with Breach Att'y 13 (Jan. 7, 2022).

could result in waiver.[253] Sometimes they even cited the potential for such requests as an independent reason not to produce a report in the first place. As with insurers, lawyers claimed that they were willing to orally answer purely factual questions from the auditor.[254]

Different results obtained for breaches involving credit card data, where firms were contractually required to permit an investigation resembling an audit. The Payment Card Industry Data Security Standard ("PCI DSS") requires a Payment Card Industry ("PCI") certified vendor to conduct an investigation, which must then be shared with the payment cards council.[255] Interestingly, this consideration motivated the dual-track investigation structure infamously used by Target following its 2013 breach.[256] In particular, the defense accepted that the PCI investigation was discoverable by plaintiffs, but successfully argued that a second independent investigation conducted under the supervision of counsel was protected by privilege.[257] One interviewee said this was widely misinterpreted as a viable strategy independent of a PCI investigation but in fact would not be useful in any other scenario.[258] None of the lawyers we interviewed ran a dual-track investigation primarily because it was viewed as too costly and unnecessary for the purposes of protecting privilege.[259] Ultimately, no interviewees endorsed dual-track investigations as a strategy to improve confidentiality protections.

---

253. *See, e.g.*, Zoom Interview with Breach Att'y 12 (Jan. 7, 2022); *see also* R. Alexander Swider, *Toeing the Line: The Delicate Balance Attorneys Must Maintain When Responding to Auditor Inquiry Request Letters*, 50 IND. L. REV. 969, 987 (2017) (reviewing caselaw showing that courts are split on whether disclosure to auditors of documents results in waiver of attorney-client or work-product protections); Ricardo Colón, *Caution: Disclosures of Attorney Work Product to Independent Auditors May Waive the Privilege*, 52 LOY. L. REV. 115, 116 (2006).

254. One lawyer would ask the auditors "[W]hat do you want to know?" Zoom Interview with Breach Att'y 12 (Jan. 7, 2022). He then received a question about whether the system containing financial records was compromised, and he said no without providing further evidence. *Id.*

255. *See* PCI SEC. STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) PCI FORENSIC INVESTIGATOR (PFI) PROGRAM GUIDE 2, 5, https://listings.pcisecuritystandards.org/documents/PFI_Program_Guide_v3.0.pdf [https://perma.cc/4CL6-A93C]. *See generally* Abraham Shaw, *Data Breach: From Notification to Prevention Using PCI DSS*, 43 COLUM. J.L. & SOC. PROBS. 517, 557 (2010) (providing overview of Payment Card Industry Data Security Standard).

256. *See supra* note 191.

257. *See In re* Target Corp. Customer Data Sec. Breach Litig., No. 14-2522, 2015 WL 6777384, at *1 (D. Minn. Oct. 23, 2015).

258. Zoom Interview with Breach Att'y 20 (Jan. 5, 2022).

259. *See id.*; Zoom Interview with Breach Att'y 19 (Jan. 5, 2022); Zoom Interview with Breach Att'y 16 (Jan. 5, 2022).

4. Supply Chain Partners

In circumstances where one firm holds another firm's information or provides IT services to it, a breach at one firm can significantly impact their clients and customers.[260] For this reason, firms' commercial partners sometimes request information about a breach; sometimes this information sharing is contractually mandated and time-bound. External counsel must then balance the value of the business relationship against the risk of waiving privilege by divulging too much information. As with insurers, a common strategy is to provide periodic confidential and oral stripped-down, fact-based updates to partners about the incident at that point in time, acknowledging that the investigation is ongoing.[261] To the extent that such updates were documented rather than provided orally, respondents acknowledged that those documents would not be privileged.[262] Providing these updates on a request-by-request basis could still limit the risk that they would be shared more widely.

IV. ALIGNING CONFIDENTIALITY PROTECTIONS AND CYBERSECURITY

Lawyers' efforts to preserve the confidentiality of incident response are driven principally by the stated goal of limiting litigation risk to breached firms.[263] Yet empirical studies show that the vast majority of cyber incidents are not litigated,[264] a trend that is likely to continue given the rise of ransomware attacks[265] that may not result in the release of private information. Even among the limited number of breaches that do result in litigation, a relatively small fraction reach the discovery stage due to the distinctive procedural hurdles these cases

260. *See* JOSEPHINE WOLFF, YOU'LL SEE THIS MESSAGE WHEN IT IS TOO LATE: THE LEGAL AND ECONOMIC AFTERMATH OF CYBERSECURITY BREACHES 117–19 (2018). *See generally* GREGORY C. RASNER, CYBERSECURITY AND THIRD-PARTY RISK: THIRD PARTY THREAT HUNTING (2021) (exploring various strategies firms can take to limit the risk that they will be subject to an attack via a third party with whom they have a commercial relationship).

261. Zoom Interview with Breach Att'y 4 (Jan. 6, 2022).

262. *Id.*

263. *See supra* Section III.B.

264. *See* Sasha Romanosky, David Hoffman & Alessandro Acquisti, *Empirical Analysis of Data Breach Litigation*, 11 J. EMPIRICAL LEGAL STUD. 74, 85 (2014); Jay P. Kesan & Linfeng Zhang, *When Is a Cyber Incident Likely to Be Litigated and How Much Will It Cost? An Empirical Study*, 27 CONN. INS. L.J. 530, 537 (2021). Both the prospect of litigation and its potential costs, moreover, are well understood to depend on several factors observable at the outset of a breach, including the potential compromise of personal financial information, firm size, firm type, number of breached records, and incident type. *See* Romanosky et al., *supra*, at 91; Kesan & Zhang, *supra*, at 547–48.

265. *See* Erin Kenneally, *Ransomware: A Darwinian Opportunity for Cyber Insurance*, 28 CONN. INS. L.J. 165, 167 (2021).

face involving issues like establishing standing.[266] And, as Part II suggests, judges overseeing these cases often refuse to treat materials generated during incident response as privileged or otherwise exempt from discovery.[267] In sum, lawyers frequently appear to place undue emphasis on the potential benefits of their efforts to preserve the confidentiality of breach response.

This conclusion seems especially apt for the law firms that specialize in breach response and receive most of their cases through cyberinsurers. Although these firms were the most committed to preserving the confidentiality of incident response,[268] their cases typically involve relatively small incidents that are less likely to result in significant litigation costs.[269] Given that a small number of law firms dominate this space,[270] their undue focus on limiting litigation risk can plausibly be interpreted as an effort to entrench their own market power. Focusing on litigation risk and legal rules governing confidentiality allows these lawyers to preserve their business model, notwithstanding their limited technical sophistication.[271]

Irrespective of the potential benefits of these efforts to preserve the confidentiality of breach response, Part III demonstrated that they have high costs. Lawyers' focus on confidentiality is holding back the formal evidence base about the causes of cyber incidents and limiting the understanding of key third parties in the cybersecurity ecosystem like insurers and regulators. Perhaps most perversely, it denies internal IT teams the knowledge and information they need to better understand what remediations they should implement, advocate for more security resources, and assess their long-term cybersecurity progress.

For these reasons, this Part explores potential reforms that would shift incident-response strategies toward addressing technical risk rather than litigation risk. Section A begins by analyzing prior efforts to expand the legal assurances of confidentiality associated with firms' cybersecurity efforts. These reforms, it suggests, are both over- and under-inclusive in addressing the central problems described in Part II.

---

266. *See* McGeveran, *supra* note 3, at 1144–45; Romanosky et al., *supra* note 264, at 76; Kesan & Zhang, *supra* note 264, at 564–65 (noting that overall dismissal rate of cybersecurity suits is high). *See generally* Solove & Citron, *supra* note 3, at 739 (discussing standing issues associated with data breach litigation).

267. *See supra* Section II.A.

268. *See supra* Section III.C.

269. *See* NETDILIGENCE, CYBER CLAIMS STUDY 2020 REPORT 10 (2020), https://netdiligence.com/cyber-claims-study-2020-report [https://perma.cc/CB4U-VVSP] (noting that costs of litigation are significantly larger for larger firms than smaller firms).

270. Prior work has shown that just four law firms have the majority of relationships with cyberinsurers; notably, one firm is on eighty percent of the panels in the study's sample. *See* Woods & Böhme, *How Cyber Insurance Shapes Incident Response: A Mixed Methods Study*, *supra* note 51, at 15.

271. To the extent this characterization is accurate, it suggests that these lawyers may be operating under a conflict of interest. *See generally* Richard A. Epstein, *The Legal Regulation of Lawyers' Conflicts of Interest*, 60 FORDHAM L. REV. 579 (1992).

For that reason, Section B builds on these prior proposals to offer a new set of reforms. It suggests that firms should be provided with broad protections against the prospect that their specific breach response efforts will be used against them in subsequent litigation. System designers should implement these reforms through enhanced privilege and altered evidentiary rules. At the same time, Section B argues that breached firms should be required to publicly disclose standardized information that could be used by regulators and plaintiffs alike. By disentangling the incident-response process from the production of information that can be used to hold firms accountable for failing to take appropriate precautions, we aim to remove barriers to effective incident response while preserving incentives for firms to take cybersecurity seriously.

A. Limitations of Prior Reform Proposals

Although our study is the first to empirically examine how confidentiality concerns impact breach response, commentators and policymakers have long speculated about this issue. In doing so, they have developed various proposals for reforming the legal rules involving the confidentiality of breach response. This Section describes two sets of reforms and evaluates them based on the empirical evidence described in Part III. The first would create a new cybersecurity privilege, while the second — which has been implemented in two narrow settings by federal law — limits any liability or risk of waiver for disclosing cybersecurity information to specific federal actors. Although both approaches have merit, they also have significant limitations in addressing the ways that confidentiality concerns undermine cybersecurity.

1. A Cybersecurity Privilege

Attorneys are not the only professionals whose interactions with clients are privileged. To the contrary, courts routinely treat communications between individuals and their doctors, spouses, religious advisors, and even auditors as privileged.[272] In each case, these privileges aim to balance encouraging honest and frank communication between

272. *See* Amanda H. Frost, *Updating the Marital Privileges: A Witness-Centered Rationale*, 14 WIS. WOMEN'S L.J. 1, 6–10 (1999); Lisa Vicens & Daniel D. Queen, *Audits and Adversaries: Making Disclosures to Your Auditors Without Waiving Your Privilege*, CLEARLY GOTTLIEB (May 1, 2017), https://clearymawatch.com/2017/05/audits-adversaries-making-disclosures-auditors-without-waiving-privilege/ [https://perma.cc/9T7T-46MB].

individuals and trusted advisors or loved ones with making relevant evidence available in litigation.[273]

With that in mind, two prominent commentaries — one from Professor Kosseff and the other from the Sedona Report — have suggested that courts or lawmakers should recognize a new "cybersecurity privilege."[274] Both proposals envision a broad-ranging privilege extending to communications between cybersecurity professionals and their clients regarding preparing for or responding to cybersecurity threats.[275] Moreover, both proposals employ a "functional" definition of who would qualify as a cybersecurity professional.[276]

The differences between the two cybersecurity privilege proposals are also notable. For instance, the Sedona Report envisions a more qualified privilege than Professor Kosseff's proposal, which, like the work-product doctrine, would permit discovery when parties could demonstrate a substantial need for the materials and an inability to acquire them through alternative means.[277] Additionally, the Sedona Report suggests that parties claiming the privilege should be required to sufficiently document their reasons for doing so to allow opposing parties to challenge that claim.[278] Perhaps most notably, the Sedona Report suggests a no-waiver rule when firms disclose privileged information to criminal law enforcement authorities investigating an attack.[279]

Both proposals have merit. They would allow companies to more quickly and flexibly respond to suspected cybersecurity threats without hiring a lawyer or being forced to engage in formalistic — and time-consuming — routines to increase the chances of attorney-related privileges applying.[280] And they would also provide companies with enhanced certainty that any efforts to document their incident response

---

273. *See* RESTATEMENT (THIRD) OF THE L. GOVERNING LAWS. § 68 cmt. c (AM. L. INST. 2000); Jaffee v. Redmond, 518 U.S. 1, 7 (1996) ("The Court of Appeals qualified its recognition of the privilege by stating that it would not apply if, 'in the interests of justice, the evidentiary need for the disclosure of the contents of a patient's counseling sessions outweighs that patient's privacy interests.'" (quoting Jaffee v. Redmond, 51 F.3d 1346, 1357 (7th Cir. 1995))).

274. *See* Kosseff, *supra* note 24, at 285–303; *Sedona Report*, *supra* note 24, at 99–100.

275. *See* Kosseff, *supra* note 24, at 285–303; *Sedona Report*, *supra* note 24, at 99–100.

276. For instance, Kosseff suggests that, rather than applying to professionals with specific security-related certifications, the privilege should apply to all "professionals engaged in the protection of communications systems and networks, and the information contained therein" so that a "firm's cybersecurity-related audit work would be protected from discovery." Kosseff, *supra* note 24, at 300; *see also Sedona Report*, *supra* note 24, at 99–100 (proposing a privilege that would apply whenever a "person or its representative" provides advice concerning "(i) a cybersecurity threat or (ii) that person's actual or potential actions in anticipation of or in response to a cybersecurity threat").

277. *Sedona Report*, *supra* note 24, at 98–100.

278. *See id.* at 100–01. The Sedona Report also suggests that its proposed privilege be implemented via legislation rather than common law to enhance certainty and uniformity. *See id.* at 107–08.

279. *See id.* at 114–18.

280. *See id.* at 105.

would not be discoverable in subsequent litigation.[281] As suggested in Part III, litigation risk has substantially reduced incident-response documentation, a result that has undermined accountability among cybersecurity professionals, efficient internal allocation of cybersecurity resources, and long-term knowledge generation both within breached firms and across the wider community.[282]

At the same time, both cybersecurity privilege proposals are, in our view, over- and under-inclusive in addressing the principal problems created by lawyers' efforts to promote the confidentiality of firms' cybersecurity efforts. The over-inclusivity of both proposals stems from the fact that they would extend not only to post-breach incident-response efforts, but also to pre-breach efforts to minimize the risk of a cybersecurity incident. Yet our findings in Part III do not, we believe, provide sufficient support for concluding that confidentiality concerns significantly impair firms' pre-breach cybersecurity efforts.[283] To the contrary, almost all of the interviewees we spoke to suggested that confidentiality concerns only minimally impact firms' pre-breach cybersecurity efforts, notwithstanding the fact that attorney-client privilege and work-product protections rarely extend to this domain.[284] Even in the isolated counter-examples we heard, the effects were generally limited to occasional routing of these efforts through attorneys and editing of cybersecurity professionals' work product.[285]

For this reason, the over-inclusivity of prior cybersecurity privilege proposals would unduly limit available information to potential plaintiffs and regulators regarding firms' pre-breach cybersecurity efforts. In doing so, they would undermine the capacity of law and regulation to hold firms accountable for their failure to adopt reasonable cybersecurity precautions.[286] Additionally, they could lead to efforts by firms to involve cybersecurity consultants in their ordinary computer operations, such as the production of computer-generated logs or automated vulnerability scans, so as to shield them from potential discovery.[287] Even worse, these cybersecurity proposals could have the perverse

281. *See* Kosseff, *supra* note 24, at 284.

282. *See supra* Section III.B.

283. Interestingly, the Sedona Report itself seems to acknowledge that extending a privilege to pre-breach activities rests on the "contestable assumption that the risk of disclosure in litigation creates disincentives for entities to develop robust and effective cybersecurity policies and practices." *Sedona Report*, *supra* note 24, at 96. This is ultimately an "empirical question." *Id.*

284. *See supra* Section III.B.2.

285. *See supra* Section III.B.2.

286. *See* SOLOVE & HARTZOG, *supra* note 1, at 190–98; Hurwitz, *supra* note 13, at 1520 (explaining that "law, when working well, can create powerful incentives that align individual conduct with socially-optimal goals" when it comes to cybersecurity).

287. *Sedona Report*, *supra* note 24, at 98–99 (recognizing that this would be a bad outcome). While the Sedona Report's documentation and justification requirements might be sufficient to address this risk, much would depend on how rigorous those justifications were in practice, as well as the ability of courts to understand and challenge them.

effect of discouraging firms from engaging in such ordinary cybersecurity activities without the assistance of third-party consultants who could provide privilege, thus introducing an artificial cost overhead to all cybersecurity activities.

Prior cybersecurity privilege proposals are under-inclusive as well. In particular, neither proposal would address prevailing concerns about breached firms or their lawyers sharing breach-related information with third parties.[288] On the contrary, both proposals seem to envision that ordinary waiver rules would apply to their proposed cybersecurity privileges, at least outside of unusual circumstances.[289] The only exception is that the Sedona Report would create a limited no-waiver rule for information sharing with criminal law enforcement officials.[290] Ironically, however, Part III suggested that many lawyers and firms currently feel comfortable sharing oral information with law enforcement, and that this information is typically sufficient for these officials to do their job.[291] Meanwhile, Part III also illustrated that firms' unwillingness to share breach-related information with their insurers, auditors, supply chain partners, and regulators can substantially impair cybersecurity by undermining the ability of these stakeholders to learn the causes of incidents and prevent them in the future.[292]

2. Information Sharing with the Federal Government

The information-sharing reforms that have gained the most traction in cybersecurity to date attempt to limit the risks of sharing information about cybersecurity incidents with the federal government. The most important example is the Cybersecurity Information Sharing Act of 2015.[293] Under CISA, firms enjoy certain protections when they share "cyber threat indicators" and "defensive measures" for a "cybersecurity purpose."[294] These include protections from liability and waiver of any privileges for sharing such information.[295] However, these protections are subject to a host of limitations and caveats.[296] For instance, liability

288. *See supra* Section III.D.

289. *See* Kosseff, *supra* note 24, at 298–303; *Sedona Report*, *supra* note 24, at 108–24 (proposing a limited no-waiver rule, but only for criminal investigations).

290. *Sedona Report*, *supra* note 24, at 114–18.

291. *See supra* Section III.D.2.

292. *See supra* Sections III.D.1, III.D.3, III.D.4.

293. 6 U.S.C. §§ 1500–10. *See generally* Brad S. Karp, *Federal Guidance on the Cybersecurity Information Sharing Act of 2015*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Mar. 3, 2016), https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/ [https://perma.cc/8A7E-2RN5].

294. 6 U.S.C. § 1503(c)(1).

295. *See id.*; 6 U.S.C. §§ 1504(d)(1), 1505(b)(1).

296. *See generally* Jamil N. Jaffer, *Carrots and Sticks in Cyberspace: Addressing Key Issues in the Cybersecurity Information Sharing Act of 2015*, 67 S.C. L. REV. 585 (2016).

protections under CISA generally[297] only apply when firms share information with the federal government through a specific Department of Homeland Security ("DHS") process.[298] Similarly, CISA only limits waiver of privilege when firms disclose information through this federal DHS process.[299] In either case, moreover, these protections only attach if firms follow a complex set of requirements within CISA that include, for instance, scrubbing personal information and implementing certain security controls.[300]

In addition to CISA, Congress recently passed the Cyber Incident Reporting for Critical Infrastructure Act of 2022.[301] Unlike CISA, CIRCIA mandates reporting to DHS of cybersecurity incidents involving critical infrastructure, a category that includes firms operating in financial services, telecommunications, information technology, healthcare, and energy sectors.[302] As with CISA, CIRCIA includes assurances that disclosures made under the law will not result in liability or waiver of otherwise applicable privileges.[303]

Although these provisions in CISA and CIRCIA may encourage breached firms to share information about incidents with the federal government,[304] they do little to address most of the broader problems described in Part III. The scope of these laws is narrow, applying only to specific types of threat intelligence, certain classes of cybersecurity incidents, and specific government offices.[305] Moreover, they do nothing to promote information sharing between breached firms and private

---

297. CISA does also extend liability protections for "communications by a regulated non-Federal entity with such entity's Federal regulatory authority regarding a cybersecurity threat." 6 U.S.C. 1504(c)(1)(B)(ii).

298. 6 U.S.C. 1504(c).

299. *See* 6 U.S.C. 1504(d)(1).

300. 6 U.S.C. 1503(d).

301. Cyber Incident Reporting for Critical Infrastructure Act of 2022, 6 U.S.C. §§ 681–681g, 665j, 659.

302. *Compare* 6 U.S.C. § 652a(a)(2) (2022) (adopting the definition of "Critical Infrastructure" used in Presidential Policy Directive 21), *with* Directive on Critical Infrastructure Security and Resilience, 2013 DAILY COMP. PRES. DOC. 106 (Feb. 12, 2013). It remains to be seen whether CIRCIA's requirements and protections will lead to a significantly broader understanding of cybersecurity threats. Since it only covers information sharing with DHS, however, it is likely to be of little use to other third parties involved in cybersecurity incident response. *See* 6 U.S.C. § 681a–681g.

303. 6 U.S.C. § 681e(b)(3).

304. Even that conclusion is unclear. As suggested above, the various complexities, requirements, and carveouts contained within CISA do not necessarily make it strategically sensible for firms to share sensitive cybersecurity information with DHS. *See* Jaffer, *supra* note 296, at 587, 595; Kristin N. Johnson, *Managing Cyber Risks*, 50 GA. L. REV. 547, 582–83 (2016). This is particularly true given that information sharing with the federal government can result in proprietary information inadvertently being revealed. *See* Derek E. Bambauer, *Secrecy Is Dead — Long Live Trade Secrets*, 93 DENV. L. REV. 833, 845 (2016).

305. 6 U.S.C. § 1501(6) (articulating the specific classes of cyber threat indicators); 6 U.S.C. § 681(8) (using the same definition for "cyber threat indicator" as CISA). *But see* 6 U.S.C. § 681(4) (allowing the CISA director to define the scope of a "covered cyber incident" through rulemaking procedures).

actors — including insurers, auditors, and supply chain partners.[306] Nor do they even do much to encourage information sharing with firms' state and federal regulators.[307] And even when it comes to information sharing with the federal government, these laws do not fundamentally address firms' concerns that any information they share in this manner could be used in a lawsuit against them that was unrelated to the decision to share.[308] For CISA and CIRCIA to address this concern, they would not only have to protect against lawsuits related to the sharing of information, but they would also have to prevent the shared information from being discovered by plaintiffs in other lawsuits.

Even more, CISA and CIRCIA are not designed to promote breached firms' own efforts to document and remedy cybersecurity incidents;[309] instead, by focusing solely on disclosure of breach information rather than its production,[310] they seem to assume that breach response documentation functions work reasonably well. Yet to the extent that breached firms avoid documenting and thoroughly investigating cybersecurity breaches, any disclosure of this information to federal actors, or anyone else, will be correspondingly diminished in its helpfulness.

B. Disentangling Incident Response and Breach Disclosure

If firms are to elevate cybersecurity goals over litigation risk in breach response, they must be assured that doing so will not substantially increase their litigation, reputational, or regulatory risks. Yet merely cloaking breach response with broad confidentiality protections risks undermining accountability for firms that fail to implement reasonable cybersecurity precautions in advance of a breach. It could also serve to further inhibit efforts by insurers and policymakers to aggregate and analyze large-scale data about the effectiveness of cybersecurity controls and best practices for protecting data and networks.

This Section proposes a pathway for navigating the conflicting goals of promoting cybersecurity while preserving accountability by disentangling the incident-response process from the production and disclosure of information to enforcement authorities and potential plaintiffs. Building on the cybersecurity privilege proposals described above, this Section first focuses on reforms that could assure firms that robust breach response documentation, communication, and

306. *See supra* Section III.D.

307. Some of CISA's protections do extend to certain communications to federal regulators. *See* 6 U.S.C. § 1505.

308. *See, e.g.*, 6 U.S.C. § 1504(d)(1) (implementing a no-waiver rule for disclosures under CISA, but leaving the remainder of evidence law intact); 6 U.S.C. § 681e(b)(3) (same).

309. *See supra* Sections III.B, III.C.

310. *See, e.g.*, 6 U.S.C. § 1503(c)(1); 6 U.S.C. § 681b(1)(A) (covering required reporting under CIRCIA); 6 U.S.C. § 681c(a) (covering voluntary reporting under CIRCIA).

information sharing would not meaningfully increase their litigation, regulatory, or reputational risks. It then explores pathways for reforming accountability mechanisms for breached firms in ways that are independent of those firms' breach response processes.

1. A Cyber-Incident Response Privilege and Evidentiary Restriction on Subsequent Remedial Measures

A revised version of the cybersecurity privilege proposed by Kosseff and the Sedona Report could go a long way toward providing breached firms with the assurances they need to prioritize their own cybersecurity and that of society more broadly in breach response. We propose that state and federal lawmakers create a nonwaivable Cyber-Incident Response Privilege. Unlike prior proposals, this privilege would not attach to any pre-incident cybersecurity measures given the limited evidence we uncovered that confidentiality concerns in this setting are distorting firms' cybersecurity efforts,[311] as well as the potential unintended consequences such a privilege could create.[312] Instead, as its name suggests, the Cyber-Incident Response Privilege would only shield firms' incident-response efforts from discovery.

Our proposed Cyber-Incident Response Privilege would thus be both narrower and stronger than prior proposals in crucial ways. First, building on the nonwaiver terms of CISA and CIRCIA, the proposed privilege would not be treated as waived if breached firms or their representatives voluntarily shared breach response information with any other third party, including insurers, regulators, supply chain partners, or auditors.[313] This provision is necessary to induce breached firms to share information with these third parties. Even more importantly, it is necessary to allow third parties like insurers and auditors to insist on information sharing as a condition of their continued relationship (for auditors or supply chain partners) or claims payments (for insurers) with a breached firm.

Second, the Cyber-Incident Response Privilege would extend beyond communications between breached firms and cybersecurity professionals to cover internal communications to technical staff within the breached firm. In doing so, the privilege would depart from conventional privileges, which generally only apply to communications between firms and outside professionals.[314] This departure is, in our view,

311. *See supra* Sections III.B, III.C.

312. *See supra* Section IV.A.1.

313. Some circuit courts have held that disclosure of privileged information to certain government actors does not operate as a waiver of privilege as to plaintiffs, a principle known as selective waiver. *See* Colin P. Marks, *Corporate Investigations, Attorney-Client Privilege, and Selective Waiver: Is a Half-Privilege Worth Having at All?*, 30 SEATTLE U. L. REV. 155, 165 (2006).

314. *See supra* Section II.A.

sensible because a primary cybersecurity goal should not only be to encourage full and frank communication between firm personnel and outside parties like lawyers or cybersecurity firms, but also to encourage full and frank internal communication within breached firms. Moreover, as Part III vividly illustrated, making cybersecurity-related privileges turn on the involvement of third parties of any type can substantially distort the breach response process as firms angle to trigger legal assurances of confidentiality. Allowing the privilege to be triggered by an event — a breach — rather than by the identity of the responding parties avoids that very real problem.

A Cyber-Incident Response Privilege would substantially encourage breached firms to prioritize cybersecurity over other goals in their breach response efforts. First, it would allow firms to select breach response coordinators based on their leadership and technical abilities rather than based on a state-sponsored privilege uniquely extended to a specific profession. In some cases, this may result in breached firms continuing to opt for lawyers as breach response coordinators. In other cases, firms may prefer that technical experts coordinate breach response. Second, a Cyber-Incident Response Privilege would encourage broad and fully informed breach response across the personnel of impacted firms. Third, it would encourage firms to fully document their breach response efforts, including commissioning the production of complete incident-response reports by cybersecurity firms.

Finally, a Cyber-Incident Response Privilege would enable insurers and regulators to demand access to documentation related to cyber-incident investigations by limiting any concern that acceding to these demands would result in waiver. Such information sharing would strengthen the ability of third parties to aggregate useful datasets about cybersecurity controls and countermeasures. It would also improve the general knowledge about the most effective means of securing computer networks and data. For instance, insurers could mandate that their policyholders produce incident reports and provide those reports as part of any cyber-related claim without fear that doing so might open their policyholders up to additional liability in the event of a lawsuit. This possibility is real: our interviews with insurers suggest that at least some carriers might be interested in stepping into that role.[315]

An alternative — or potentially even an additional — approach to promoting broader cybersecurity goals in firms' incident-response efforts is to create an evidentiary rule limiting the admissibility in civil actions of firms' efforts in breach response. Such a rule could be patterned on Federal Rule of Evidence 407, which substantially limits the

315. Insurers also noted that their ability to do this would depend on their market power and whether other insurers were taking similar steps. *See, e.g.*, Zoom Interview with Insurer 1 (Jan. 20, 2022).

admissibility of measures "taken that would have made an earlier injury or harm less likely to occur."[316] The goal of that rule is to encourage firms to take remedial measures in furtherance of physical safety, such as repairs, installation of safety devices, and changes in company rules.[317] Under the rule, such efforts cannot permissibly be used to support an inference that the firm acted improperly in connection with an initial harm.[318] Extending this type of evidentiary rule to the breach response could well achieve many of the same goals, limiting the potential concern that a firm's breach response efforts will be used to show that the firm's pre-breach cybersecurity measures were inadequate.

One advantage of the Cyber-Incident Response Privilege over a modification to the rules of evidence is that it can potentially be applied more broadly to materials like entire incident reports. Incident reports may, for instance, include descriptions of measures that the breached firm did not ultimately take following a breach; those may not be protected by the evidentiary rule. So, the evidentiary rule alone may constrain what can be included in reports, especially long-term recommendations, which firms may not implement in the immediate aftermath of an incident.

By contrast, the advantage of the evidentiary rule would be that it applies to certain facts that the Cyber-Incident Response Privilege may not cover, such as whether the firm implemented specific security controls in the aftermath of a breach. While that information might be included in a final report, courts might view it as falling outside the purview of privilege because whether or not a company enables multifactor authentication or password requirements would be factual information.[319] Accordingly, the strongest protections to ensure that firms are incentivized to both produce thorough documentation of investigations and take immediate remediation steps might be a combination of the proposed cyber-incident privilege and the proposed evidentiary rule.

2. Reforming Information Sharing

Reforming confidentiality or evidentiary rules alone, without further changes to the existing incident-response process, could impair accountability for breached firms. In particular, shielding firms' breach response efforts from discovery or admissibility would mean that regulators and plaintiffs would have less capacity to hold firms

316. FED. R. EVID. 407.

317. *See* FED. R. EVID. 407 advisory committee's note on proposed rules.

318. FED. R. EVID. 407.

319. *See generally* Paul R. Rice, *Attorney-Client Privilege: Continuing Confusion About Attorney Communications, Drafts, Pre-Existing Documents, and the Source of the Facts Communicated*, 48 AM. U. L. REV. 967, 979–83 (1999).

accountable for failing to take reasonable cybersecurity precautions. We take this concern seriously, notwithstanding that most breaches do not result in litigation or regulatory action and that litigation has a low percentage of success when it is brought.[320] This is partly because the very threat of such legal or regulatory action can have a substantial deterrent effect, particularly if the underlying substantive rules regarding liability are well-designed. Additionally, even limited legal and regulatory actions in the past have produced important principles about firms' cybersecurity obligations that can have a broader positive effect.[321]

One way to preserve accountability while reforming confidentiality protections would be to extend the existing reporting requirements to a broader range of firms and incidents. For instance, the mandatory incident-response reporting contained in CIRCIA requires reporting of cybersecurity incidents by certain critical infrastructure operators only to DHS.[322] Extending these reporting obligations[323] to all severe cybersecurity incidents, not just those affecting critical infrastructure, would be a significant step toward mitigating the risk that breached entities might not investigate these incidents or document those investigations properly.

Still, in such a model, the breached firm collects and curates details about the incident. As a result, all analyses not run and data not collected are lost to time. This dynamic is precisely why the Payment Card Industry Data Security Standard requires that a certified investigator conduct an investigation to establish facts.[324]

---

320. *See* McGeveran, *supra* note 3, at 1144–45; Romanosky et al., *supra* note 264, at 76; Kesan & Zhang, *supra* note 264, at 564–65.

321. *Cf.* Solove & Hartzog, *supra* note 13, at 666–76; Christopher Bradley, *Privacy for Sale*, 40 YALE J. ON REG. 127, 189–92 (2023).

322. 6 U.S.C. § 681b(a)(1)(A).

323. CIRCIA requires reporting to DHS of cybersecurity incidents by certain critical infrastructure operators including:

"(A) A description of the covered cyber incident, including —

(i) identification and a description of the function of the affected information systems, networks, or devices that were, or are reasonably believed to have been, affected by such cyber incident;

(ii) a description of the unauthorized access with substantial loss of confidentiality, integrity, or availability of the affected information system or network or disruption of business or industrial operations;

(iii) the estimated date range of such incident; and

(iv) the impact to the operations of the covered entity.

(B) Where applicable, a description of the vulnerabilities exploited and the security defenses that were in place, as well as the tactics, techniques, and procedures used to perpetrate the covered cyber incident.

(C) Where applicable, any identifying or contact information related to each actor reasonably believed to be responsible for such cyber incident.

(D) Where applicable, identification of the category or categories of information that were, or are reasonably believed to have been, accessed or acquired by an unauthorized person."
6 U.S.C. § 681b(c)(4).

324. *See* PCI SEC. STANDARDS COUNCIL, *supra* note 255, at 2.

A second and more ambitious model might build on the PCI DSS to establish a mandatory forensic evidence collection pipeline entirely distinct from incident response. Private firms could coordinate this process, or the obligation could be placed on independent technology providers.[325] Given the ease of replicating digital evidence, this process could seek to preserve server logs, disk images, files, and other forensic evidence, which would be turned over to plaintiffs' attorneys as part of the discovery process. This data-collection infrastructure would additionally support forensic investigators hired by the breached firm because this type of evidence is now inconsistently collected.

Another variant of this more ambitious model would require firms that experience a sufficiently serious breach to use specific automated forensic tools to preserve evidence for use in a subsequent lawsuit or enforcement action. Rather than dumping raw data, platform providers could be required to integrate analytical capabilities that produce semi-automated reports. For example, one forensic provider demonstrated a tool that produced investigative reports for compromised Office 365 email inboxes.[326] This approach might benefit regulators and plaintiffs' attorneys, who may lack the expertise to use raw technical information to conduct their own investigations.

Both of these proposals — expanding CIRCIA or establishing a mandatory, automated evidence collection pipeline — would represent a significant shift in the rules governing cyber-incident reporting in the United States. Currently, such reporting requirements, at both the state and federal level, remain fairly minimal, requiring that certain types of incidents, such as the breach of personal identifying information, be reported, but not requiring the inclusion of many details about how those incidents were perpetrated or what steps were taken to remedy them.[327]

V. CONCLUSION

All of the lawyers, forensic investigators, and insurers we spoke to acknowledged that concerns about attorney-client privilege and confidentiality affected their work on cybersecurity incidents in ways that spanned the short-term response to such incidents, the ex ante preparation for them, and the longer-term collection of robust data sets and knowledge about online threats and effective countermeasures. Our interviews suggest that the uncertainty surrounding the applicability of attorney-client privilege and work-product protection to post-breach

325. For consistency purposes, this forensic evidence would ideally be automatically collected and preserved through technical tools such as Microsoft's Computer Online Forensic Evidence Extractor for extracting evidence from Windows devices.

326. *See* Zoom Interview with Forensic Investigator 3 (Dec. 14, 2021).

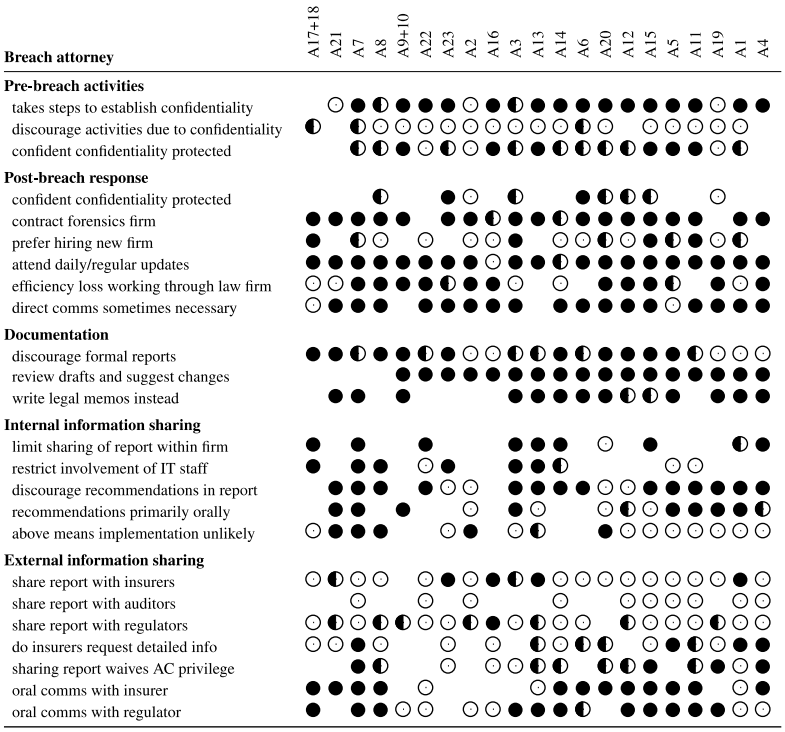
327. *See* Vaaler & Greenwood, *supra* note 22, at 27.

cybersecurity investigation materials has exacerbated these problems by slowing the pace of investigations, causing lawyers to discourage the documentation of incident causes and technical recommendations, and leading to less candid security assessments with clear industry benchmarks. As one interviewee succinctly put it, "[t]he trajectory of the law is doing a disservice to cybersecurity."[328] Addressing these significant obstacles to both short- and long-term cybersecurity necessitates greater clarification and tailoring of incident response confidentiality protections. To accomplish this, we suggest expanding these confidentiality protections to enable swifter responses to incidents, more robust documentation of breaches, and broad sharing of this information with interested third parties. Pairing these enhanced confidentiality protections with new requirements to collect and share forensic evidence and analysis can ensure that law and regulation continue to hold firms accountable when they fail to invest in adequate security protections before a breach occurs.

328. Zoom Interview with Breach Att'y 12 (Jan. 7, 2021).

APPENDIX A

Table 1: Strategies employed by each breach attorney (A1–A23) that we interviewed.



●/○ = participant supported/contradicted the statement in the first column, ◐ = the participant described nuance (e.g. "it depends on…"), and no symbol if we were not confident of the participant's belief upon reviewing the transcript. A9+10 and A17+18 were joint interviews. The column order is generated from a dendrogram to cluster similar response patterns.